Facultad de Ingeniería

Ingeniería de Sistemas e Informática

Programa Especial de Titulación

Implementación de acceso remoto al personal de la ONPE para realizar Teletrabajo mediante la herramienta Forticlient VPN

Autor: Josué Antony Leyva Cabrera

Para obtener el Título Profesional de

Ingeniero de Sistemas e Informática

Asesor: Genns Eduardo Yataco Silva

Lima – Perú

2021

INDICE DE CONTENIDO

INDICE DE FIGURAS **4**
INDICE DE TABLAS **5**
INTRODUCCION **6**
CAPITULO 1 ..... **7**
ASPECTOS GENERALES **7**
1.1. Definición del Problema 7
1.1.1. Descripción del Problema 7
1.1.2. Formulación del Problema 8
1.1.2.1.Problema General 9
1.1.2.2. Problemas Específicos 9
1.2. Definición de objetivos 9
1.2.1. Objetivo general 9
1.2.2. Objetivos específicos 9
1.3. Alcances y limitaciones 9
1.3.1. Alcances 9
1.3.2. Limitaciones 10
1.4. Justificación 10
CAPITULO 2 ..... **11**
MARCO TEÓRICO **11**
2.1. Fundamento teórico 11
2.1.1.Estado del Arte 11
2.1.2. Base Teórica 12
2.2. Marco conceptual 13
2.3 Marco Metodologico 15
CAPITULO 3 ..... **166**
DESARROLLO DE LA SOLUCIÓN **166**
3.1.Caso de Negocio 16
3.2.Gestión del Proyecto 17
3.2.1.Enunciado del Alcance 17
3.2.1.1.EDT/WBS 20
3.2.2.Gestión del Tiempo 21
3.2.3.Gestión del Costo 23
3.2.3.1.Estimación del Costo del Proyecto 23
3.2.3.1.1.Costo de Personal 23

3.2.3.1.2.Costo de Hardware 23
3.2.3.2.Flujo de Caja 24
3.2.3.3.Valor Ganado 25
3.2.4.Gestión de la Calidad 26
3.2.5.Gestión de la Comunicación 28
3.2.6.Gestión de Riesgos 29
3.2.7.Gestión de Interesados 31
3.2.8.Gestión de Adquisiciones 33
3.2.9.Cierre del Proyecto 33
3.3.Desarrollo del Proyecto 36
CAPITULO 4 59
RESULTADOS 59
4.1. Resultados 59
4.2. Presupuesto 60
CONCLUSIONES 61
BIBLIOGRAFÍAS 62

INDICE DE FIGURAS

Figura 1. Árbol del Problema..... .8
Figura 2. Organigrama. 17
Figura 3. EDT ..... .20
Figura 4. Gestión del Tiempo. 21
Figura 5. Diagrama de Gantt. ..... .22
Figura 6. Probabilidad vs Impacto..... .29
Figura 7. Diagrama Topológico. ..... .38
Figura 8. Características del Fortinet Fortigate 800D. ..... .39
Figura 9. Fortinet Fortigate 800D. ..... .40
Figura 10. Interface de inicio de sesión. ..... .41
Figura 11. Contenido Fortigate ..... .41
Figura 12. LDAP Server ..... .42
Figura 13. RADIUS Servers ..... .42
Figura 14. SSL VPN Portals..... .43
Figura 15. SSL VPN Settings..... .43
Figura 16. Política de acceso..... .44
Figura 17. User Groups..... .44
Figura 18. User Definition..... .45
Figura 19. Configuración desktop Windows ..... .45
Figura 20. Desactivar estado de suspensión..... .46
Figura 21. Configuración desktop Mac OS..... .46
Figura 22. Agregar usuario de dominio en Mac OS ..... .46
Figura 23. Instalación Forticlient VPN (1) ..... .47
Figura 24. Instalación Forticlient VPN (2) ..... .47
Figura 25. Instalación Forticlient VPN (3) ..... .48
Figura 26. Instalación Forticlient VPN (4) ..... .48
Figura 27. Instalación Forticlient VPN (5) ..... .49
Figura 28. Token Fortinet..... .49
Figura 29. Conexión a Escritorio remoto. ..... .50
Figura 30. Credenciales de dominio para ingreso a Windows..... .50
Figura 31. Ingreso remoto a Windows. ..... .51
Figura 32. VNCViewer..... .51
Figura 33. Credenciales de dominio para ingreso a VNCViewer..... .51
Figura 34. Credenciales de dominio para ingreso a Mac OS..... .52
Figura 35. Ingreso remoto a Mac OS..... .52
Figura 36. Validación de acceso remoto en el Monitor del Fortigate..... .53
Figura 37. Validación de acceso remoto para el personal de ONPE..... .59

INDICE DE TABLAS

Tabla 1. Cuadro de Causa y Efecto. 8
Tabla 2. Enunciado del Alcance 17
Tabla 3. Costo de Personal. 23
Tabla 4. Costo de Hardware. 23
Tabla 5. Flujo de Caja. 24
Tabla 6. Valor Ganado. 25
Tabla 7. Control de calidad 26
Tabla 8. Gestión de la Comunicación. 28
Tabla 9. Gestión de Riesgos. 30
Tabla 10. Registro de interesados y nivel de involucramiento. 31
Tabla 11. Matriz de Adquisiciones. 33
Tabla 12. Acta de cierre del Proyecto.. 33
Tabla 13. Acta de Conformidad 35
Tabla 14. Informe actual de la red 36
Tabla 15. Equipos por local. 37
Tabla 16. Usuarios por local. 37

INTRODUCCION

La Oficina Nacional de Procesos Electorales actualmente en el marco de la situación de estado de emergencia por el COVID-19 solo se puede realizar trabajo remoto, la institución no cuenta con una herramienta que permita el acceso remoto lo cual impide al personal desarrollar sus actividades con normalidad, retrasando el cronograma de actividades.

En el presente proyecto se evaluó una solución para este problema: implementar una herramienta VPN para dar acceso remoto al personal de ONPE y así pueda desarrollar sus actividades de manera eficiente y segura.

En este sentido, en el primer capítulo de la presente investigación, se desarrollará la definición del problema, el objetivo general, alcances, limitaciones y justificación, el segundo capítulo está referido en el sustento teórico de la tesis, el marco teórico aborda el fundamento teórico, estado del arte y base teórica, marco conceptual y marco metodológico.

El tercer capítulo se presenta el desarrollo de la solución el cual contiene la implementación del acceso remoto, el caso de negocio, la gestión del proyecto y toda la documentación correspondiente. Finalmente, en el cuarto capítulo se detallará los resultados obtenidos del proyecto implementado, conclusiones y recomendaciones.

CAPITULO 1

ASPECTOS GENERALES

1.1. Definición del Problema

1.1.1. Descripción del Problema

La Oficina Nacional de Procesos Electorales es un organismo electoral constitucional autónomo que formar parte del Estado, es la máxima autoridad encargada de ejecutar y organizar los distintos procesos electorales del país, entre referéndum y otras consultas populares. Para ello vela para obtener la libre expresión de la voluntad popular, los cuales se llevan a cabo en los procesos electorales.

Por la carencia de una herramienta informática de acceso remoto que ocasiona al personal de ONPE no poder desarrollar sus actividades con normalidad en medio del estado de emergencia por el COVID-19, el cual impide realizar trabajo presencial y solo remoto.

En ese sentido se propone implementar la herramienta Forticlient VPN para dar acceso remoto al personal de ONPE y así pueda desarrollar el cronograma de actividades, entre ellas las elecciones internas 2020 y las elecciones generales 2021.

Aplicando el árbol de problema se identifican las causas y los efectos que existen dentro de la institución, (Ver Figura 1 y Tabla 1).

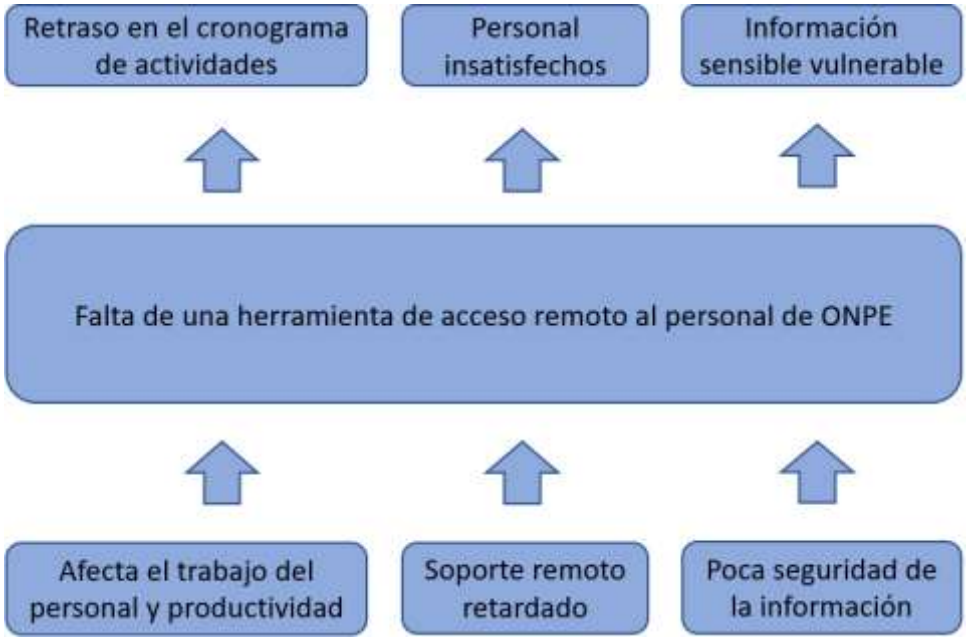


Figura 1. Árbol del Problema

Fuente: Elaboración propia.

Tabla 1. Cuadro de Causa y Efecto.

Causa	Efecto
1. Afecta el trabajo del personal y productividad	Retraso en el cronograma de actividades
2. Soporte remoto retardado	Personal insatisfechos
3. Poca seguridad de la información	Información sensible vulnerable

Fuente: Elaboración propia.

1.1.2. Formulación del Problema

El problema central del proyecto es que la ONPE no cuenta con una herramienta tecnología para el acceso remoto, bajo este contexto se hace una formulación la siguiente pregunta:

- ¿En qué medida la implementación de acceso remoto al personal de la ONPE permite realizar teletrabajo mediante la herramienta Forticlient VPN?

1.1.2.1. Problema General

Falta de una herramienta de acceso remoto para el personal de ONPE.

1.1.2.2. Problemas Específicos

- Incumplimiento con el cronograma de actividades.
- No poder realizar teletrabajo.
- No poder dar soporte remoto.
- Personal en riesgo de contagio por el COVID-19 y costo de transporte.

1.2. Definición de objetivos

1.2.1. Objetivo general

Implementar el acceso remoto al personal de la ONPE para realizar teletrabajo mediante la herramienta Forticlient VPN.

1.2.2. Objetivos específicos

- Determinar una política de acceso remoto a la red para la implementación del acceso remoto Forticlient VPN.
- Determinar la arquitectura tecnología para implementar el acceso remoto Forticlient VPN.
- Instalar y configurar la herramienta Forticlient VPN que mediante la implementación nos permitirá controlar los ordenadores de los usuarios.
- Dar servicio de soporte tecnológico a través de la implementación de la herramienta Forticlient VPN.
- Desarrollar un Manual de conexión para la implementación de la herramienta Forticlient VPN.

1.3. Alcances y limitaciones

1.3.1. Alcances

Se implementará una VPN que será configurada con un dispositivo de seguridad Fortinet y se aprovechará la disponibilidad del directorio activo de la organización.

Se definirá una política de acceso remoto a la red.

Se definirá la arquitectura a utilizar en la implementación de la VPN.

Se configurará e integrará el firewall con el directorio activo.

Se configurará e implementará políticas de firewall para la conectividad de los usuarios VPN.

Se desarrollará para las sedes de Lima.

Se desarrollará un manual de conexión a la VPN.

1.3.2. Limitaciones

Esta limitado al presupuesto establecido.

1.4. Justificación

La presente investigación a través de la implementación del acceso remoto busca el beneficio al personal de la ONPE que en el marco de la situación de estado de emergencia actual se está trabajando de forma remota a causa del COVID-19, por ese motivo se quiere evitar que el personal se enferme y baje la producción, afectando el cronograma de actividades, también buscar mejorar los tiempos de atención, pues dado la problemática del estado de emergencia y toque de queda, limita al personal trabajar de forma remota.

En ese sentido i) en lo social beneficia al personal, pues al trabajar desde su hogar lo hace de forma segura, como así reducir el estrés y mejorar la eficiencia, ii) en lo económico reducir los gastos de transporte, combustible, energía eléctrica y equipos, y iii) en lo tecnológico mejorar los tiempos de atención y calidad de servicio.

CAPITULO 2

MARCO TEÓRICO

2.1. Fundamento teórico

2.1.1. Estado del Arte

En este capítulo se presenta los antecedentes nacionales e internacionales del sector público y privado, relativos a la presente investigación.

Mar en su tesis propone como objetivo general “Elaborar la propuesta de implementación de una intranet vía VPN, para mejorar la confidencialidad del intercambio de información entre las sedes Lima y Cusco del INEI”. (Mar, 2016, pág. 21). Por lo tanto, la información el personal administrativo es vulnerable al no contar con una seguridad, encriptación mediante una VPN. Además, el autor en su investigación concluye que “Se simuló el intercambio de información por medio del servidor de correos entre las cuentas alina@inei.com y CarlosPerez@inei.com (clientes VPN), dando como resultado una comunicación exitosa entre ambas cuentas” (Mar, 2016, pág. 110). Por lo tanto, la implementación de una intranet VPN logró el intercambio de información entre las sedes de forma segura.

Siguiendo en esta línea de investigación, Ramírez, Jota y Penagos en su tesis proponen como objetivo general “Diseñar una red privada virtual (VPN) con seguridad de protocolo de túnel de capa dos, para la empresa Laboratorios EXPOFARMA S.A”. (Ramírez, Jota y Penagos, 2019, pág. 8). Por lo tanto, la data de la empresa EXPOFARMA S.A. es vulnerable y no segura, al diseñar la VPN con seguridad L2TP hace el viaje de la data segura y confiable. Además, el autor ha demostrado como una conclusión que “el diseño de este proyecto amplio la posibilidad de que los empleados pudieran continuar desarrollando sus labores diarias aun cuando están fuera de la compañía” (Ramírez, Jota y Penagos, 2019, pág. 38. En ese sentido el diseño de la red privado virtual logró la conexión remota para sus empleados sin verse afectados en sus actividades.

Por su parte Peña propone como objetivo general “Diseñar e implementar una red privada virtual (VPN SSL) utilizando el método de autenticación LDAP en una empresa privada”. (Peña. 2016, pág. 24). Por lo tanto, la implementación de esta VPN permitirá a los empleados poder establecer una conexión segura para poder manipular información sensible de la organización. Además, Peña concluye que una política de acceso remoto a la red Organizacional, en la cual se indica el uso apropiado de la conexión remota (VPN SSL) hacia la red de la organización, y se aplica a todos los empleados y consultores externos que hagan uso de esta forma de conexión. (Peña, 2016, pág.81).

2.1.2. Base Teórica

2.1.2.1. Acceso remoto

El acceso remoto es la acción de conectarse a aplicaciones, datos de TI o servicios desde una distinta ubicación a la sede de trabajo u otra ubicación más cercana al centro de datos Por lo que es la capacidad de acceder a un ordenador o dispositivo desde otro dispositivo en cualquier momento y desde cualquier lugar. (Citrix, 2019)

Para ello hay varias tecnologías de seguridad para el acceso remoto seguro, que incluyen:

- **Red privada virtual**: se establece una conexión a través de una red existente, generalmente Internet pública, los cuales están protegidos con autenticación y encriptación
- **Inicio de sesión único** : permite que un usuario autenticado acceda a aplicaciones seleccionadas con un conjunto inicial de credenciales de inicio de sesión.
- **Uso compartido de escritorio**: proporciona a un usuario acceso en tiempo real a archivos y datos ubicados en otro dispositivo. (ciberseguridad,2020)

2.1.2.2. Teletrabajo

El teletrabajo es una forma de trabajo a distancia que beneficia tanto al empleador como al trabajador, y a la sociedad a largo plazo, protegiendo el medio ambiente. Esto es posible gracias a las tecnologías de la información y comunicación, y se puede emplear en el hogar del trabajador u otros establecimientos diferentes al hogar del empleador. (argentina, 2020)

El teletrabajo comenzó a ponerse en práctica en la década de los años 70 del siglo XX en EEUU. El físico Jack Niles fue el que empezó a pensar en una forma en la que los trabajadores pudieran desarrollar sus tareas sin la necesidad de asistir a las oficinas de la empresa.

Durante ese tiempo el desarrollo tecnológico no estaba demasiado avanzado, y fue algo que no se pudo llevar a cabo plenamente hasta décadas posteriores.

El avance de las nuevas tecnologías permitió que muchas empresas se dieran cuenta de que gracias a ello se podían ahorrar costes y optimizar recursos.

Las empresas se han dado cuenta de que trabajar de forma remota les permite ahorrar en costes, y además evitar los desplazamientos de los trabajadores contribuye a una mejora en el medio ambiente evitando el gasto de combustible que implicaría que se llevasen a cabo cada día esos desplazamientos a la oficina.

Hay que tener en cuenta los siguientes parámetros para poder desarrollar un correcto trabajo dentro de esta opción: la tecnología debe ser la requerida, la conectividad es fundamental a la hora del desarrollo ya que el teletrabajo se basa mayoritariamente en el uso de las nuevas tecnologías. Será positivo formar a los trabajadores en rutinas, pautas y consejos para llevar a cabo esta forma de trabajar de manera óptima. (economipedia, 2020)

2.2. Marco conceptual

2.2.1. VPN

El VPN es una tecnología que se utiliza para conectar diferentes equipos a una red privada usando internet, los beneficios que brinda son:

- **Autenticación**: Establecer una conexión segura es un problema complicado que se resuelve con una serie de matemáticas ingeniosas en un proceso denominado autenticación.
- **Tunelización**: Las VPN también protegen la conexión entre el cliente y el servidor utilizando tunelización y encriptación.
- **Encriptación**: Los datos dentro del túnel también son encriptados de tal manera que solo el destinatario previsto puede desencriptarlos. (expressvpn, 2020)

2.2.1. Fortinet

El Fortinet de es una compañía pionera en integrar varias funciones en una sola plataforma de Gestión Unificada de Amenazas. Esta plataforma incluye: antivirus, control de aplicaciones, cortafuegos, VPN, prevención de intrusos y filtrado web, para otorgar una protección total a tus contenidos. Funciona bajo el enfoque de mantener seguras las redes corporativas de una forma unificada, amplia, integrada y automatizada.

Las bondades que ofrecen son las siguientes:

- **Seguridad de red**: Al proteger con seguridad avanzada todas las ubicaciones de tu empresa.
- **Acceso Seguro**: Ofrece acceder a aplicaciones y dispositivos de forma segura, sin comprometer el rendimiento.

- **Seguridad física y virtual**: Por medio del uso de dispositivos inteligentes, cuyas características físicas y de programación les sirve para detectar, prevenir y responder ante cualquier amenaza.
- **Protección de dispositivos**: Al proporcionar un monitoreo proactivo de los equipos, a fin de controlar su funcionamiento en toda la red.
- **Seguridad de aplicaciones**: Garantizado mediante un software que es capaz de detectar y detener amenazas en avanzada.

2.2.1. Fortigate

El Fortigate es la plataforma bandera de Firewall de Fortinet, la cual está disponible para diferentes tipos de organizaciones. Esta plataforma es adaptable a cualquier entorno empresarial, sin perder sus funciones de seguridad de última generación, también es conocido como el dispositivo de seguridad más famosos de Fortinet. (vertical-ibérica, 2020)

- **Firewall:** Toda la línea de equipos permite definir individualmente cada una de las interfaces y así darle la posibilidad al equipo a configurar las WAN o DMZ permitiendo trabajar en las interfaces para realizar escaneo de virus, filtro de ip o monitoreo del tráfico.
- **Control de aplicaciones**: El Control de Aplicaciones provee un control altamente granular sobre las aplicaciones, llegando incluso hasta identificar al usuario individual que está haciendo uso de ella.
- **Reportes Flexibles:** La obtención de reportes disponibles en los equipos FortiGate, permitiendo poder realizar auditorías.
- **VPN IPsec / SSL V**PN: El FortiOS cuenta con la posibilidad de crear VPN IPSec y SSL, el cual permite configurar un portal para que los usuarios ingresen y se conecten. (z-net, 2019)

2.3. Marco Metodológico

2.1.3. Tipo de Investigación

El método del enfoque es cuantitativo porque se propone dar resultados al implementar una herramienta para el acceso remoto. Además, según Sampieri (2017) “El enfoque cuantitativo (que representa, como dijimos, un conjunto de procesos) es secuencial y probatorio” (p. 4).

2.1.4. Nivel de Investigación

De acuerdo con la naturaleza del estudio se tiene un alcance Explicativo porque según Sampieri (2017) “Los estudios explicativos van más allá de la descripción de conceptos o fenómenos, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales” (p. 95).

2.1.5. Diseño de la Investigación

El método es no experimental porque según autor Sampieri (2017) “se trata de estudios en los que no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar para analizarlos” (p. 152).

A continuación, se indica las fases por las cuales se ejecutará el proyecto:

Fase 1: Levantamiento de información, análisis de la empresa, se recopila información como informe actual de la red, el hardware disponible y cantidad de usuarios.

Fase 2: Diseño de la plataforma tecnológica, con el fin de implementar la solución, se realiza el diagrama topológico, un plan de configuración y especificaciones para la VPN, de acuerdo a los requerimientos y necesidades.

Fase 3: Configuración e implementación de la VPN, en esta fase se realizará desde la instalación, configuración e integración del Firewall del Fortigate 800d hasta la autenticación con Radius, pruebas de conexión y manual de configuración.

CAPITULO 3

DESARROLLO DE LA SOLUCIÓN

3.1. Caso de Negocio

La Oficina Nacional de Procesos Electorales actualmente en el marco de la situación de estado de emergencia por el COVID-19 solo se puede realizar trabajo remoto, la institución no cuenta con una herramienta que permita el acceso remoto lo cual impide al personal desarrollar sus actividades con normalidad, retrasando el cronograma de actividades.

Por lo que el presente proyecto busca implementar una herramienta informática de acceso remoto VPN al personal de la ONPE para que así puedan desarrollar sus actividades según el cronograma, entre ellas las elecciones internas 2020 y las elecciones generales 2021.

Entre objetivos estratégicos tenemos:

- Que al cabo de la implementación el 90% del personal este trabajando de forma remota.
- Que se cumpla al 100% el cronograma de actividades y se cumpla con las elecciones.

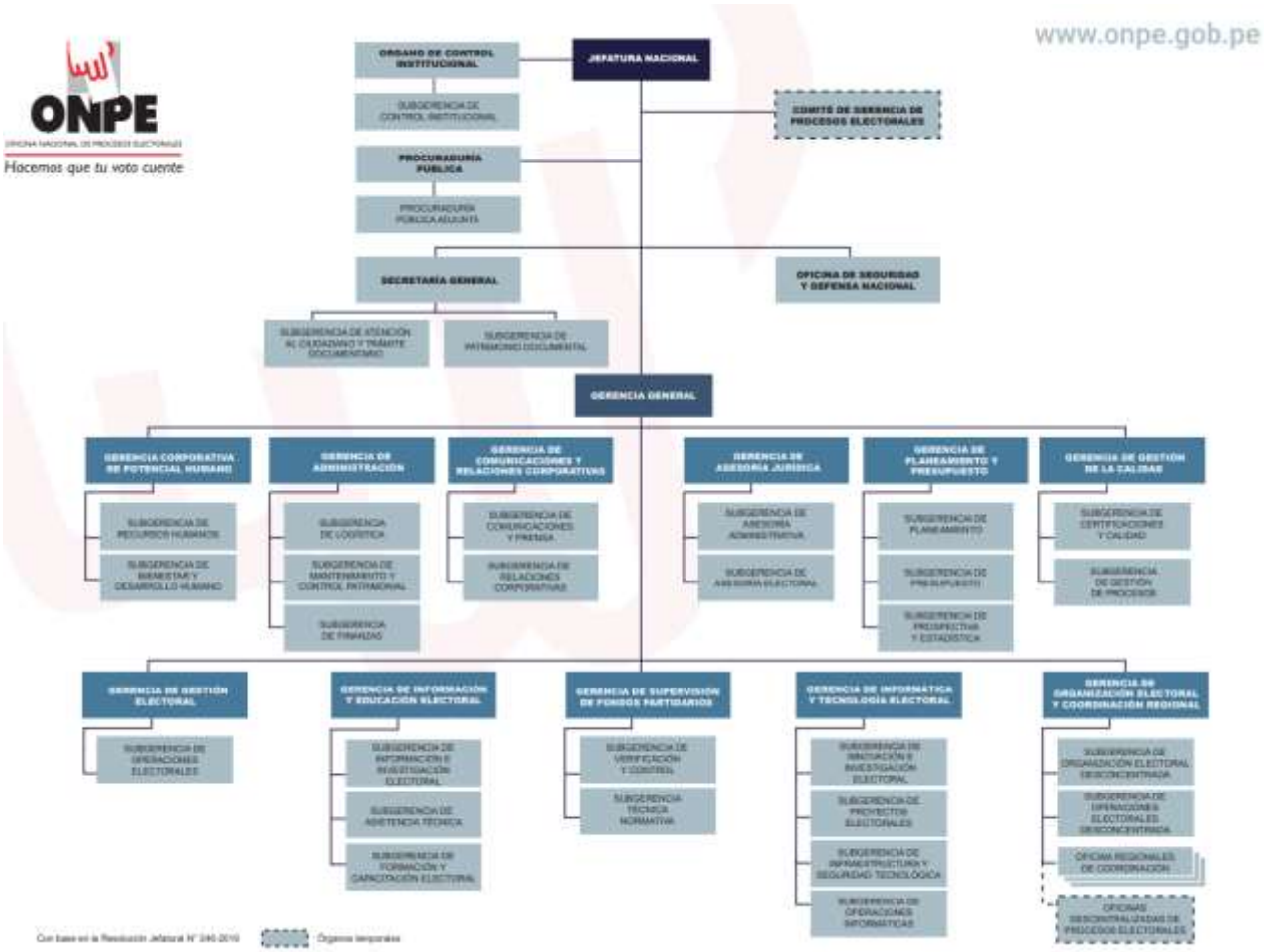


Figura 2. Organigrama.
Fuente: Elaboración propia.

3.2. Gestión del Proyecto

La gestión del proyecto se compone de la gestión de alcance, gestión de tiempo, gestión de costos, gestión de calidad, gestión de comunicaciones, gestión de adquisiciones, gestión de riesgos y registro de interesados.

3.2.1. Enunciado del Alcance

En esta sección se presenta el enunciado del alcance del proyecto, el cual se muestra de manera detallada la descripción del proyecto y del producto. Se ha tomado en cuenta los entregable principales, los criterios de aceptación y las exclusiones, (Ver Tabla 2).

Tabla 2. Enunciado del Alcance

1.OBJETIVO DEL PROYECTO
Implementar el acceso remoto al personal de la ONPE para realizar teletrabajo mediante la herramienta Forticlient VPN.

2.DESCRIPCIÓN DEL ALCANCE DEL PROYECTO

El proyecto tiene como alcance la implementación de acceso remoto al personal de la institución para realizar teletrabajo, dicho proyecto contribuirá en el desarrollo de actividades y en la seguridad del personal, puesto que estando en un estado de emergencia solo está permitido el trabajo remoto.

3.REQUERIMIENTOS DEL PROYECTO

1 Fortinet fortigate 800d
1 Jefe de proyecto
1 Ingeniero de redes
2 técnicos en redes
2 soporte técnicos
Firewall
Herramienta forticlient VPN

4.REQUERIMIENTOS DEL PRODUCTO

Análisis

- Informe actual de la red: el cual nos permite determinar las características de la arquitectura de la red.
- Informe de Hardware locales: el cual nos permite saber con cuantos equipos desktop disponibles cuenta la institución para el acceso remoto.
- Informe de Usuarios por local: determinar la cantidad de usuarios por local mediante el directorio activo.

Diseño

- Diagrama topológico propuesta: nos proporciona un mapa visual que muestra cómo está conectada la red para la implementación.
- Plan de configuración y especificaciones VPN: configuración del Fortinet de acuerdo a las necesidades para la implementación y especificaciones VPN para el acceso remoto.
- Requerimientos y necesidades del pedido: documento que detalla los requerimientos y necesidad para la implementación.

Implementación

- Instalación del Hardware Fortinet: instalación del Fortinet fortigate 800d en el gabinete del centro de datos.
- Configuración del Fortinet inicial y puesta en marcha: documentación que detalla la configuración del Fortinet para la implementación.
- Configuración con Autenticación Radius: documento de la configuración para con el directorio activo de la institución.
- Configuración del Firewall para Autenticación y bloqueo: documento de la configuración del firewall a los usuarios del directorio activo para la autenticación y restricción por políticas.
- Configuración de desktop: configuración de equipos de acuerdo al sistema operativo para el acceso remoto y desactivar la suspensión del equipo.
- Instalación del forticlient VPN: esta instalación se realizará en los equipos personales de los usuarios y será configurado con unos parámetros que permitirá el acceso remoto.
- Pruebas de red: verificación y prueba de conectividad.
- Manual de configuración VPN para usuarios: manual de ayuda que servirá de guía para la correcta conexión.

5.EXCLUSIONES DEL PROYECTO
Las exclusiones del proyecto son las siguientes: • No se realzará cambios en la estructura organizacional. • No se realizará cambios en las funciones desempeñadas y responsabilidades del personal TI.
6. ENTREGABLES DEL PROYECTO
• Gestión del proyecto: Definir el alcance, EDT, Cronograma de actividades, Estimación de costos, matriz de comunicaciones, matriz de adquisiciones, reuniones de trabajo, avance del proyecto, gestión de riesgos, registro de interesados y cierre de proyecto. • Análisis: documento de informe actual de la red, de hardware locales y de usuarios por local. • Diseño: diagrama topológico, plan de configuración y especificaciones VPN, requerimientos y necesidades. • Implementación: instalación del hardware Fortinet, configuración del Fortinet inicial y puesta en marcha, configuración con autenticación Radius, configuración del firewall para autenticación y bloqueo, configuración de los equipos desktop, instalación de la herramienta forticlient VPN, Pruebas de red y la realización de un manual de configuración VPN.
7.CRITERIOS DE ACEPTACIÓN DEL PRODUCTO
La implementación del acceso remoto se debe cumplir al 100% con los requerimientos y necesidades establecidas.
8.RESTRICCIONES DEL PROYECTO
No aplica

Fuente: Elaboración propia.

3.2.1.1. EDT/WBS

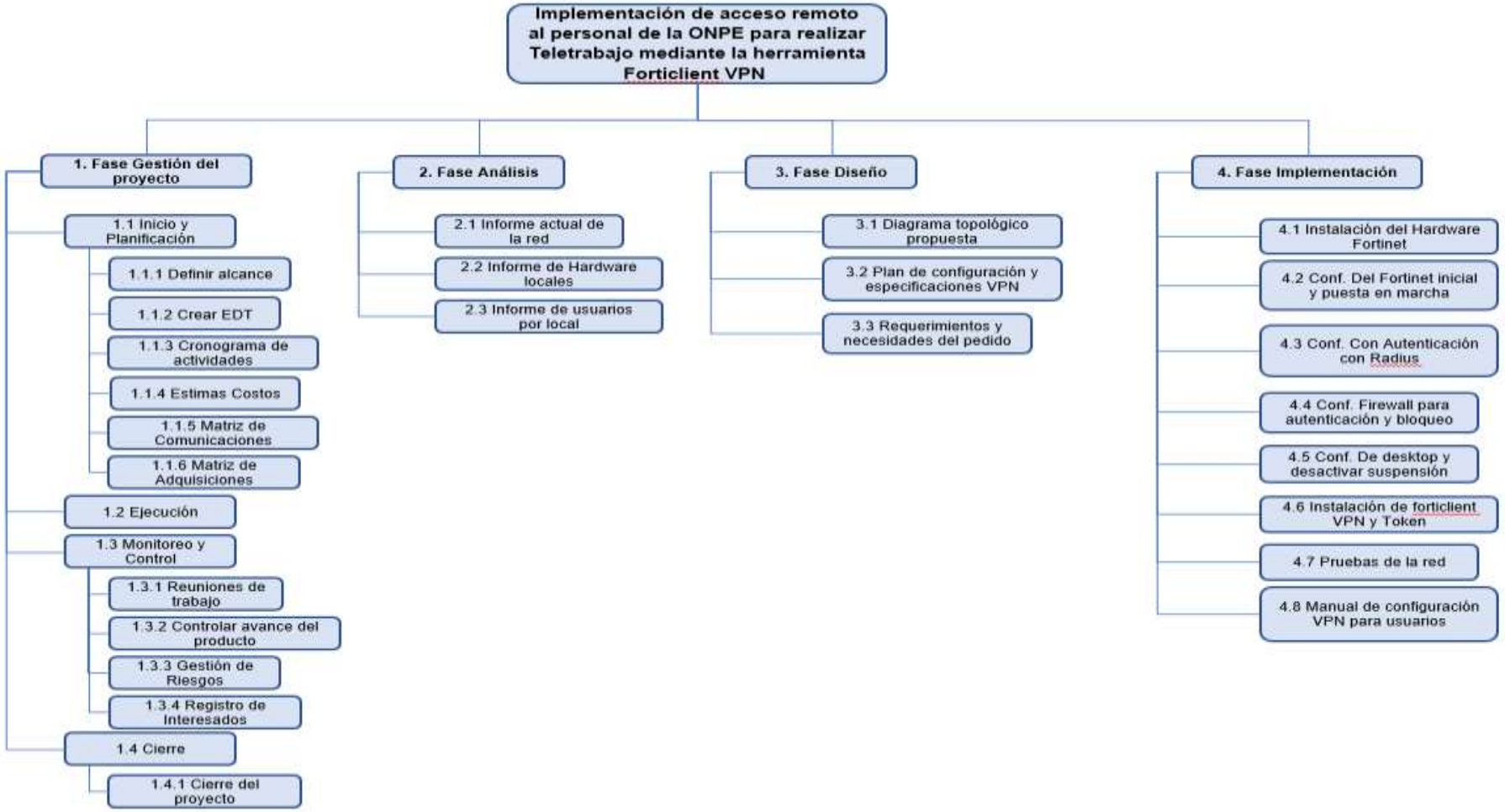


Figura 3. EDT.
Fuente: Elaboración propia.

3.2.2. Gestión del Tiempo

En esta sección se establece el tiempo necesario para garantizar que el proyecto esté en un plazo viable para implementar el acceso remoto para el teletrabajo. En ese sentido a continuación se muestra el cronograma de actividades.

Nombre de tarea	Duración	Comienzo	Fin
Implementación Acceso remoto VPN	**106 días**	**lun 12/10/20**	**jue 11/03/21**
Gestión	**19 días**	**lun 12/10/20**	**jue 5/11/20**
Inicio y Planificación	**6 días**	**lun 12/10/20**	**lun 19/10/20**
Definir alcance	1 día	lun 12/10/20	lun 12/10/20
Crear EDT	1 día	mar 13/10/20	mar 13/10/20
Elaborar cronograma de actitividades	1 día	mié 14/10/20	mié 14/10/20
Estimar Costos	1 día	jue 15/10/20	jue 15/10/20
Elaboración Matriz de Comunicaciones	1 día	vie 16/10/20	vie 16/10/20
Elaboración Matriz de Adquisiciones	1 día	lun 19/10/20	lun 19/10/20
Monitoreo y Control	**10 días**	**mar 20/10/20**	**lun 2/11/20**
Reuniones de trabajo	4 días	mar 20/10/20	vie 23/10/20
Controlar avance del producto	2 días	lun 26/10/20	mar 27/10/20
Gestión de Riesgos	2 días	mié 28/10/20	jue 29/10/20
Registro de Interesados	2 días	vie 30/10/20	lun 2/11/20
Cierre	**3 días**	**mar 3/11/20**	**jue 5/11/20**
Cerrar el proyecto	3 días	mar 3/11/20	jue 5/11/20
Análisis	**7 días**	**vie 6/11/20**	**lun 16/11/20**
Informe actual de la red	2 días	vie 6/11/20	lun 9/11/20
Informe de Hardware locales	3 días	mar 10/11/20	jue 12/11/20
Informe de Usuarios por local	2 días	vie 13/11/20	lun 16/11/20
Diseño	**11 días**	**mar 17/11/20**	**mar 1/12/20**
Diagrama Topológico Propuesta	5 días	mar 17/11/20	lun 23/11/20
Plan de Configuración y especificaciones VPN	3 días	mar 24/11/20	jue 26/11/20
Requerimientos y necesidad del pedido	3 días	vie 27/11/20	mar 1/12/20
Implementación	**69 días**	**mié 2/12/20**	**jue 11/03/21**
Instalación del Hardware fortinet	1 día	mié 2/12/20	mié 2/12/20
Configuración del fortinet inicial y puesta en marcha	2 días	jue 3/12/20	vie 4/12/20
Configuración con Autenticación Radius	2 días	lun 7/12/20	mié 9/12/20
Configuración Firewall para Autenticación y bloqueo	30 días	jue 10/12/20	vie 22/01/21
Configuración de desktop y desactivar suspensión	30 días	lun 4/01/21	vie 12/02/21
Instalación de forticlient VPN y Token	30 días	lun 25/01/21	vie 5/03/21
Pruebas de red	2 días	lun 8/03/21	mar 9/03/21
Manual de configuración VPN para usuarios	2 días	mié 10/03/21	jue 11/03/21

Figura 4. Gestión del Tiempo.
Fuente: Elaboración propia.

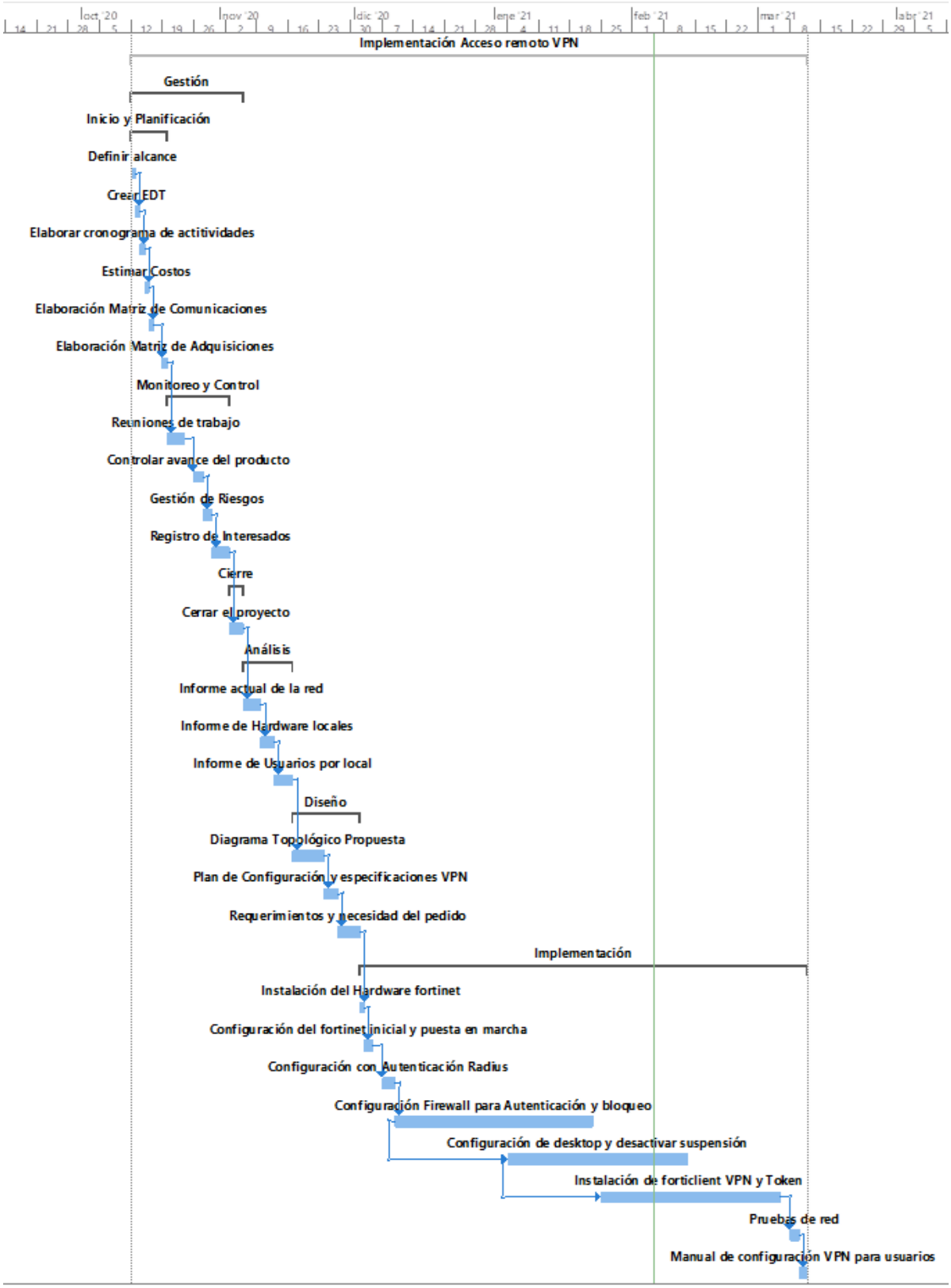


Figura 5. Diagrama de Gantt.
Fuente: Elaboración propia.

3.2.3. Gestión del Costo

La gestión de costos permite estimar, presupuestar y controlar los costos de modo que el proyecto se complete dentro del presupuesto aprobado. En ese sentido se muestra a continuación la estimación del costo del proyecto y flujo de caja.

3.2.3.1. Estimación del Costo del Proyecto

3.2.3.1.1. Costo de Personal

Se incluye a todo el personal de TI que estará involucrado en el proyecto, (Ver Tabla 3).

Tabla 3. Costo de Personal.

Perfil Personal	Cantidad (unidades)	Sueldo Mensual	Tiempo asignado (meses)	Costo Total
Jefe de Proyecto	1	S/. 9,000.00	6 meses	S/. 54,000.00
Ingeniero de redes	1	S/. 6,000.00	6 meses	S/. 36,000.00
Técnico en redes	2	S/. 4,000.00	6 meses	S/. 48,000.00
Soporte Técnico	2	S/. 3,000.00	5 meses	S/. 30,000.00
Total				**S/. 168,000.00**

Fuente: Elaboración propia.

3.2.3.1.2. Costo de Hardware

En esta parte se incluye todos los costos correspondientes al equipo que nos permite realizar el análisis, desarrollo y la implementación del acceso remoto, (Ver Tabla 4).

Tabla 4. Costo de Hardware.

Elemento	Cantidad (unidades)	Costo (unidad)	Costo Total
Fortinet fortigate 800d	1	S/. 18,200.00	S/. 18,200.00
Mantenimiento del Fortinet	1	S/. 8,000.00	S/. 8,000.00
Total			**S/. 26,200.00**

Fuente: Elaboración propia.

3.2.3.2. Flujo de Caja

En esta sección se presenta el registro de todos los ingresos y egresos a la caja a lo largo del tiempo del proyecto, (Ver Tabla 5.

Tabla 5. Flujo de Caja.

Flujo de Caja						
	Mes 1	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**
Ingresos						
Venta/Beneficios	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Egresos						
Recursos Humanos						
Jefe de Proyecto	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00
Ingeniero de redes	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00
2 técnicos en redes	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00
2 soporte Técnico	S/. 0.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00
Equipo de Computo						
Fortinet fortigate 800d	S/. 18,200.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Mantenimiento del Fortinet	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 8,000.00
Total	**S/. 41,200.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 37,000.00**
Total Acumulado	**S/. 41,200.00**	**S/. 70,200.00**	**S/. 99,200.00**	**S/. 128,200.00**	**S/. 157,200.00**	**S/. 194,200.00**

Fuente: Elaboración propia.

3.2.3.3. Valor Ganado

En esta sección se muestra la gráfica del valor ganado el cual nos permite controlar la ejecución del proyecto a través del presupuesto con el calendario de ejecución, (Ver Tabla 6).

Tabla 6. Valor Ganado.

		Año					
		Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Valor Planificado		S/ 41,200.00	S/ 29,000.00	S/ 29,000.00	S/ 29,000.00	S/ 29,000.00	S/ 37,000.00
Valor Planificado Acumulado	PV	S/ 41,200.00	S/ 70,200.00	S/ 99,200.00	S/ 128,200.00	S/ 157,200.00	S/ 194,200.00
Costo Real		S/ 38,700.00	S/ 29,000.00	S/ 29,000.00	S/ 29,000.00	S/ 29,000.00	S/ 37,000.00
Costo Real Acumulado	AC	S/ 38,700.00	S/ 67,700.00	S/ 96,700.00	S/ 125,700.00	S/ 154,700.00	S/ 191,700.00
Porcentaje de avance completado del mes	%comp	10.0%	18.0%	18.0%	18.0%	18.0%	18.0%
Valor ganado del trabajo realizado	[EV= % comp x BAC]	S/ 19,420.00	S/ 34,956.00	S/ 34,956.00	S/ 34,956.00	S/ 34,956.00	S/ 34,956.00
Valor ganado del trabajo realizado acumulado	EV	S/ 19,420.00	S/ 54,376.00	S/ 89,332.00	S/ 124,288.00	S/ 159,244.00	S/ 194,200.00

Costo total presupuestado (**BAC**)	S/ 194,200

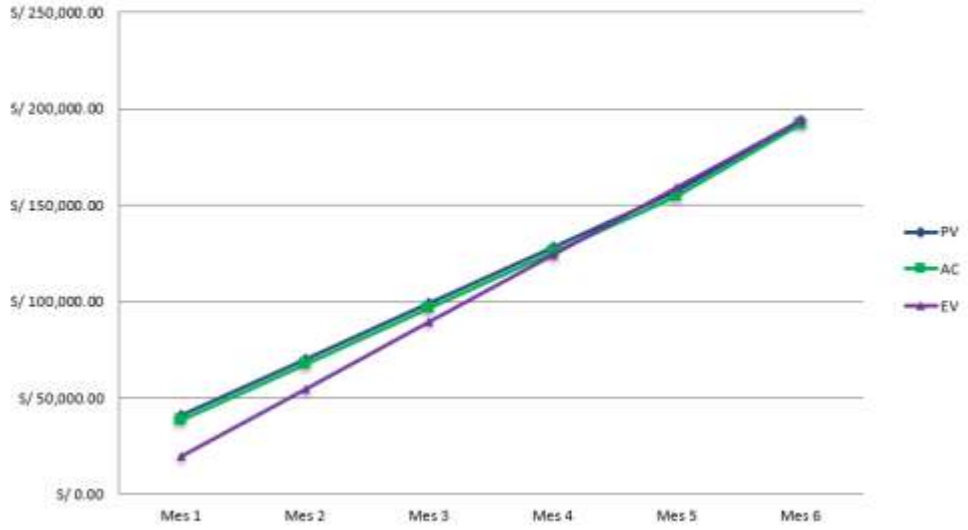
Indices y variaciones	Valor
Variación del costo (CV/Cost Variance) [**CV=EV-AC**]	S/ 2,500
Variación del cronograma (SV/Schedule Variance) [**SV=EV-PV**]	0
Índice de desempeño del costo (CPI/Cost Performance Index) [**CPI = EV/AC**]	1.01
Índice de desempeño del cronograma del proyecto (SPI/Schedule Performance Index) [**SPI = EV/PV**]	1.00
Estimación a la conclusión (EAC/Estimate at Completion) [**EAC = BAC/CPI**]	191,700

CV negativa, el proyecto está sobre gastado
CV positiva, el proyecto ha gastado menos de lo presupuestado

SV negativa, el proyecto está retrasado
SV positiva, el proyecto está adelantado

CPI menor que 1, el proyecto está sobre gastado
CPI mayor que 1, el proyecto ha gastado menos de lo presupuestado

SPI menor que 1, el proyecto está retrasado
SPI mayor que 1, el proyecto está adelantado



Fuente: Elaboración propia.

3.2.4. Gestión de la Calidad

En esta sección se establecen las estrategias que se llevaran a cabo en cada fase del proyecto para el control de la calidad, al fin de cumplir con los objetivos establecidos en el alcance del proyecto, (Ver Tabla 7).

Tabla 7. Control de calidad

Control de calidad							
Fases	**Objetivo**	**Actividades**	**Pruebas**	**Criterios de aceptación**	**Frecuencia**	**Medios de aceptación**	**Responsable**
Gestión	Asegurar el cumplimiento en cada una de las fases de la implementación del proyecto	Desarrollarlos planes de gestión: -Alcance -Tiempo -Costo -Calidad -Comunicación -Riesgos -Adquisiciones -Interesados	Evaluar avance del proyecto de acuerdo a lo establecido en la planificación	Elaboración al 100%	Varias veces de acuerdo a las fases del proyecto	Informes	-Jefe de Proyecto -Ingeniero de redes
Análisis	Asegurar el cumplimiento de elaboración de documentos como: -Informe actual de la red -Informe del hardware local -Informe de usuarios por local	-Evaluación del informe actual de la red institucional -Evaluación del informe del hardware local, equipos disponibles para el acceso remoto. -Evaluación del informe de usuarios por locales	Evaluar avance del proyecto de acuerdo a: -Alcance del producto -Cronograma de actividades	Ejecución al 100%	Una vez en la fase de Análisis	Informe de avance del proyecto	-Jefe de proyecto -Ingeniero de redes.

Diseño	Asegurar el cumplimiento de elaboración de documentos como: -Documento de Diseño -Documento del plan de configuración y especificaciones VPN	-Evaluación del documento de diseño con el diagrama topológico -Evaluación del documento del plan de configuración y políticas para la VPN	Evaluar avance del proyecto de acuerdo a: -Cronograma de actividades -Requerimientos para la implementación	Ejecución al 100%	Una vez en la fase de Diseño	Informe de avance del proyecto	-Jefe de proyecto -Ingeniero de redes. -Técnico en redes
Implementación	Asegurar el Desarrollo de la implementación	-Evaluación de avance de la implementación del acceso remoto VPN -Evaluación de avance de la configuración del fortigate 800d y autenticación con Radius -Evaluación de avance de configuración e instalación del forticlient VPN y token para el teletrabajo al personal.	Evaluar avance del proyecto de acuerdo a: -Cronograma de actividades -Requerimientos para la implementación	Ejecución al 100%	Varias veces durante la fase de Implementación	Informe de avance del proyecto	-Jefe de proyecto -Ingeniero de redes. -Técnico en redes -Soporte técnico
Estándares							
Los estándares aplicables al proyecto están basados en la norma internacional seguridad ISO 27001							

Fuente: Elaboración propia

3.2.5. Gestión de la Comunicación

En esta sección se muestra la matriz de comunicaciones la cual contiene la descripción de toda la información que se debe comunicar a los involucrados en el proyecto, (Ver Tabla 8).

Tabla 8. Gestión de la Comunicación

Fase	Contenido	Propósito	Responsable	Audiencia	Periodo	Método
Análisis	Revisión de la arquitectura actual de la red de la institución	Determinar las características de la arquitectura actual de la red	Ingeniero de redes	Equipo de desarrollo	Una vez en la fase análisis	Informe digital
	Reunión con el equipo de trabajo	Levantar información con respecto a los requerimientos para la implementación	-Jefe de proyecto -Ingeniero de redes	Equipo de desarrollo	Una vez en la fase análisis	-Reunión -Acta de reunió -Acta de requerimientos
Diseño	Elaboración del documento de diseño	Elaborar el diagrama topológico propuesto para la implementación	-Ingeniero de redes	Equipo de desarrollo	Una vez en la fase diseño	Documento digital
	Elaboración del plan de configuración y especificaciones VPN	Elaborar el plan acorde a la necesidad y requerimientos del pedido de acceso remoto	-Ingeniero de redes -Técnico en redes	Equipo de desarrollo	Una vez en la fase diseño	Documento digital
Implementación	Elaboración del desarrollo de la implementación	Elaborar la implementación en base a los requerimientos y políticas	-Ingeniero de redes -Técnico en redes	Equipo de desarrollo	Varias veces durante la implementación	Documento digital
	Elaboración de Manual de usuario	Elaborar guía de ayuda de configuración forticlient VPN para el personal	Soporte técnico	Equipo de desarrollo	Una vez al finalizar la implementación	Documento digital

Fuente: Elaboración propia

3.2.6. Gestión de Riesgos

En esta sección se mostrará la matriz de riegos con el propósito de identificar los posibles riesgos que podrían ocasionar un aumento de costos, retraso y disminución de la calidad del proyecto, (Ver tabla 9).

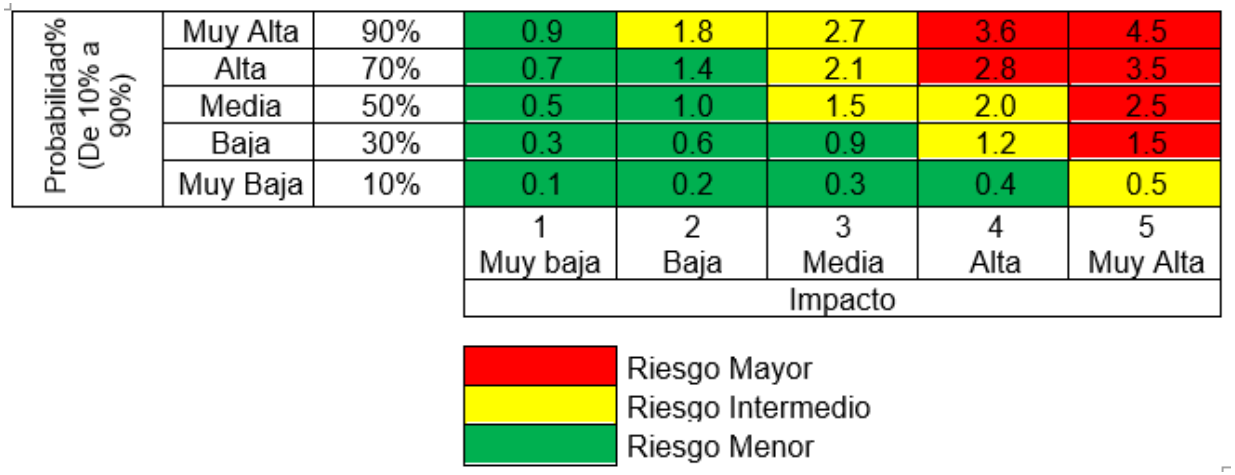


Figura 6. Probabilidad vs Impacto.
Fuente: Elaboración propia.

Tabla 9. Gestión de Riesgos

ID	Riesgo	Efecto	Probabilidad (P)	Impacto (I)	Score Riesgo (PxI)	Tipo de Riesgo	Medidas
R01	Incumplimiento en las actividades del cronograma.	Retraso considerable en el cronograma de actividades	70%	5	3.5	Riesgo Mayor	Compromiso de los involucrados recuperando el tiempo trabajando más horas o fines de semanas.
R02	Demora en la contratación de técnico en redes y soporte técnico	Retraso en la implementación del acceso remoto	30%	4	1.2	Riesgo Intermedio	Comunicación con RRHH para la pronta contratación.
R03	Poco manejo en la instalación o manejo del software forticlient VPN	Fallas o demoras en la instalación del software	30%	2	0.6	Riesgo Menor	Capacitación
R04	Daño de equipos tecnológicos	Fallas en la conexión	70%	5	3.5	Riesgo Mayor	Cambio de equipos, backup
R05	Ausencia de unos de los técnicos	Retraso en la fase de configuración de equipos	30%	4	1.2	Riesgo Intermedio	El equipo de trabajo deberá cubrir las horas
R06	Desastre natural	Paralización del proyecto ya sea por terremoto, incendio, etc.	10%	5	0.5	Riesgo Intermedio	Esperar hasta que sea seguro reanudar las actividades
R07	Usuarios no entiendo el manual de configuración forticlient VPN	Configuración y validación errónea al conectar con la red.	10%	3	0.3	Riesgo Menor	Mejorar la redacción y explicación.

Fuente: Elaboración propia

3.2.7. Gestión de Interesados

En esta sección se incluye todos los procesos necesarios para identificar a las personas, las cuales pueden estar afectadas de manera directa o indirecta en el proyecto. Por consiguiente, se presenta el registro de los interesados y su nivel de involucramiento, (Ver tabla 10).

Tabla 10. Registro de interesados y nivel de involucramiento.

ID	Nombre	Posición Organizacional	Locación	Rol en el proyecto	Información de contacto
1	Antonio Salas	Gerente de la Gerencia de Informática	Lima	Patrocinador	asalas@onpe.gob.pe
2	Pedro Gutiérrez	Oficina de proyectos y desarrollo	Lima	Jefe de Proyecto	pgutierrez@onpe.gob.pe
3	Juan López	Oficina de redes y comunicaciones	Lima	Ingeniero de Redes	jlopez@onpe.gob.pe
4	Luis Cavero	Oficina de redes y comunicaciones	Lima	Técnico en Redes	lcavero@onpe.gob.pe
5	Mario Casas	Oficina de redes y comunicaciones	Lima	Técnico en Redes	mcasas@onpe.gob.pe
6	Julio Bolaños	Oficina de Soporte Técnico	Lima	Soporte Técnico	jbolanos@onpe.gob.pe
7	Christian Magallanes	Oficina de Soporte Técnico	Lima	Soporte Técnico	cmagallanes@onpe.gob.pe
INFORMACIÓN DE EVALUACION					
ID	**Requisitos principales**	**Expectativas principales**	**Influencia Potencial**	**Fases del proyecto con mayor interés**	
1	Aprobar la realización del proyecto	Desarrollo del proyecto dentro del tiempo y costo planificado	Alto	Todo el proyecto	
2	Presentar informes y coordinar con el Ingeniero de redes para la implementación	Hacer seguimiento del cumplimiento del plan de proyecto	Alto	Todo el proyecto	

3	Desarrollo de la implementación	Desarrollo de la implementación según el alcance y tiempo planificado	Alto	Fase de Análisis, diseño e implementación
4 y 5	Coordinar con el ingeniero de redes los requerimientos de la implementación	Verificar que la implementación cumpla con los requerimientos solicitados	Bajo	Fase de diseño e implementación
6 y 7	Coordinar con el técnico de redes acerca de la configuración y validación	Desarrollo de la configuración de equipos, instalación de software, validación y pruebas.	Bajo	Fase de implementación

ID	**Involucrados**	**Interés de los involucrados en el proyecto**	**Evaluación de impacto**	**Estrategias potenciales para ganar soporte o reducir obstáculos**
1	Antonio Salas	Alto	Alto	Mantener informado sobre el avance del proyecto
2	Pedro Gutiérrez	Alto	Alto	Mantener buena comunicación sobre el avance del proyecto
3	Juan López	Alto	Alto	Mantener buena comunicación, llevar a cabo reuniones para ver el avance de la implementación
4	Luis Cavero	Alto	Bajo	Mantener buena comunicación, llevar a cabo reuniones para ver el avance de la implementación
5	Mario Casas	Alto	Bajo	Mantener buena comunicación, llevar a cabo reuniones para ver el avance de la implementación
6	Julio Bolaños	Alto	Bajo	Mantener buena comunicación
7	Christian Magallanes	Alto	Bajo	Mantener buena comunicación

Fuente: Elaboración propia.

3.2.8. Gestión de Adquisiciones

La gestión de adquisiciones consiste en todos los procesos necesarios para comprar productos y/o servicios necesarios para llevar a cabo el proyecto. En ese sentido a continuación se muestra la matriz de adquisiciones, (Ver tabla 11)

Tabla 11. Matriz de Adquisiciones.

Matriz de Adquisiciones						
Código EDT	**Estructura EDT**	**Tipo de Adquisición**	**Modalidad de Adquisición**	**Fechas Estimadas**		**Presupuesto**
				Inicio	**Fin**	
1	**Gestión**					
1.3	**Ejecución**					
	1 Fortinet fortigate 800d	Bienes	Licitación pública nacional	20/10/2020	05/11/2020	S/. 18,200.00
	1 mantenimiento del Fortinet	Servicio	Licitación pública nacional	01/03/2021	10/03/2021	S/. 8,000.00
TOTAL						**S/. 26,200.00**

Fuente: Elaboración propia.

3.2.9. Cierre del proyecto

El cierre del proyecto es la culminación del proceso proyectual, para esto tenemos el acta de cierre del proyecto y el acta de conformidad como se muestra a continuación, (Ver Tabla 12 y 13)

Tabla 12. Acta de cierre del Proyecto.

1. Cronograma			
Fecha de inicio Programada	12/10/2020	**Fecha Fin Programada**	11/03/2021

2. Lecciones Aprendidas

Que estando en un estado de emergencia se puede llevar a cabo un proyecto de implementación para la institución.

3. Productos Generados

Se logro realizar la implementación de acceso remoto al personal de la institución para que pueda seguir con su cronograma de actividades.

4. Beneficios Alcanzados

El 100% de los usuarios pudieron seguir sus actividades de forma remota, estando seguros desde sus hogares y previniendo el contagio del COVID-19

5. Cierre de Adquisiciones

Adquisiciones Programadas	Cantidad	Presupuesto	¿Se realizo la adquisición?	Monto Devengado	¿Se encuentra cerrada la adquisición?
1 Fortinet fortigate 800d	1	S/. 18,200.00	Si	S/. 18,200.00	Si
1 mantenimiento del Fortinet	1	S/. 8,000.00	Si	S/. 8,000.00	SI
	Presupuesto Total	**S/. 26,200.00**	Ejecución Total	**S/. 26,200.00**	

6. Documentación Generada en el proyecto

Documento	Ubicación	
	Física	Digital
Todos los documentos durante el proyecto fueron de formato digital.		X

7. Observaciones del proyecto

El proyecto se llegó a implementar con éxito en el tiempo estimado y costo estimado, el proyecto justifico la necesidad de poder conectarse remotamente para seguir con las labores con normalidad.

8. Firmas

Nombre	Cargo o Rol en el Proyecto	Elaborado / Revisado / Aprobado	Fecha	Firma
Antonio Salas	Patrocinador			
Pedro Gutiérrez	Jefe de Proyecto			
Juan López	Ingeniero de Redes			

Fuente: Elaboración propia

Tabla 13. Acta de Conformidad.

<table>
<tr><td colspan="6">I. Datos Generales:</td></tr>
<tr><td>Código proyecto:</td><td></td><td>Fecha:</td><td></td><td>Elaborado:</td><td></td></tr>
<tr><td>Proyecto:</td><td colspan="5">Implementación de acceso remoto al personal de la ONPE para realizar Teletrabajo mediante la herramienta Forticlient VPN</td></tr>
<tr><td colspan="6">II. De la conformidad:</td></tr>
<tr><td colspan="6">Se está de acuerdo y se da la conformidad.</td></tr>
<tr><td colspan="6">III. Del cierre del proyecto:</td></tr>
<tr><td colspan="6">Se da por cerrado el proyecto una vez culminado la implementación del acceso remoto VPN al personal de la institución.</td></tr>
<tr><td colspan="6">IV. Aprobación y aceptación del requerimiento</td></tr>
<tr><td colspan="3">Jefe de Proyecto</td><td colspan="3">Solicitante del Requerimiento</td></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td colspan="3">Firma:
Nombre: Pedro Gutiérrez
Cargo:</td><td colspan="3">Firma:
Nombre:
Cargo:</td></tr>
</table>

Fuente: Elaboración propia.

3.2. Desarrollo del Proyecto

En esta sección se realizará el desarrollo para la implementación mediante las fases, desde el análisis hasta su instalación y configuración.

3.2.1. Fase Análisis

En esta fase se realizará el análisis, levantamiento de información requerida para poder desarrollar la solución, para esto necesitamos estado actual de la red, cantidad de equipos y usuarios por locales.

3.2.1.1. Informe actual de la red

Todas las sedes están conectadas a la data center de la sede central, estas están segmentadas, (Ver Tabla 14).

Tabla 14. Informe actual de la red.

Local	Segmento
Central	172.16.80.0/24 10.54.20.0/24 10.56.2.0/24
Crillon	10.50.25.0/24 10.50.26.0/24 10.50.27.0/24
Industrial	10.50.24.0/24
Antares	10.50.23.0/24
Talara	10.50.21.0/24
Lurín	10.50.20.0/24
Condevilla	10.50.28.0/24

Fuente: Elaboración propia.

Todos los usuarios están en el directorio activo el cual será útil para poder configurar el acceso remoto, este directorio activo se encuentra en el 172.16.80.126.

3.2.1.2. Informe de Hardware por locales

En base al inventario informático de equipos del 2020 tenemos los siguientes equipos operativos, (Ver Tabla 15).

Tabla 15. Equipos por local.

Local	Desktop	Laptop	Total
Central	623	257	880
Crillon	344	113	457
Industrial	81	6	87
Antares	99	4	103
Talara	66	24	90
Lurín	240	568	808
Condevilla	5	9	14
TOTAL			**2439**

Fuente: Elaboración propia.

3.2.1.3. Informe de usuarios por locales

De acuerdo al directorio activo tenemos la siguiente cantidad de usuarios por locales, (Ver Tabla 16).

Tabla 16. Usuarios por local.

Local	Cantidad
Central	315
Crillon	255
Industrial	45
Antares	67
Talara	49
Lurín	187
Condevilla	0
TOTAL	**918**

Fuente: Elaboración propia.

3.2.2. Fase Diseño

En esta fase se realizará el diseño del diagrama topológico, así como el plan de configuración y especificaciones para la VPN, de acuerdo los requerimientos y necesidades del pedido.

3.2.2.1. Diagrama topológico propuesta

Para la implementación se tiene el siguiente diagrama, (Ver Figura 7).

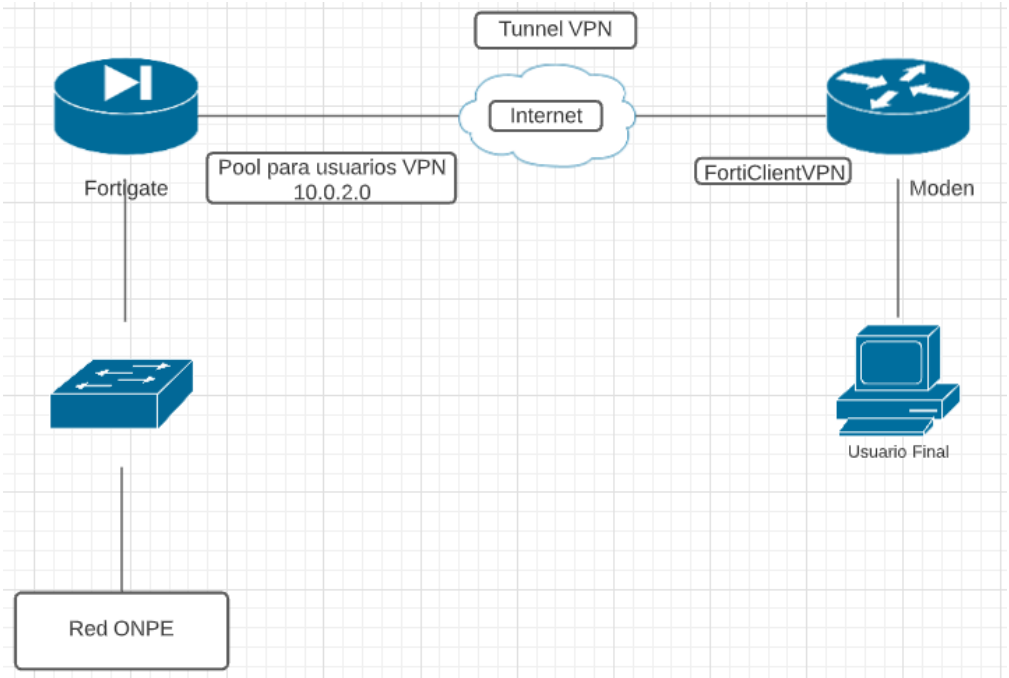


Figura 7. Diagrama Topológico.
Fuente: Elaboración propia.

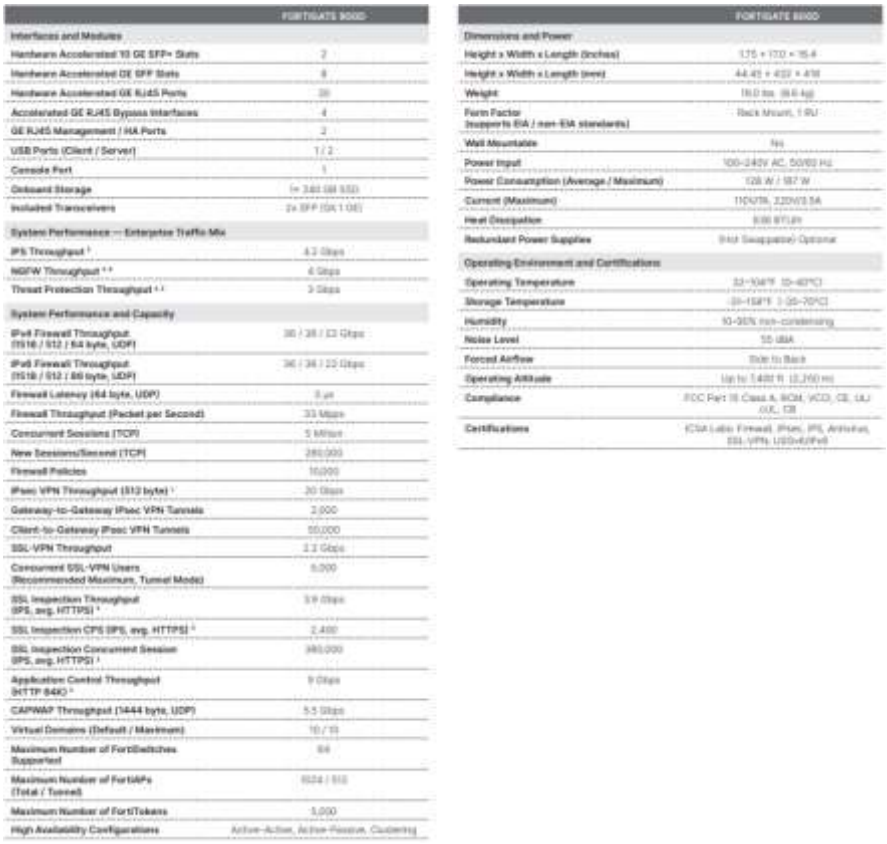
3.2.2.2. Plan de configuración y especificaciones VPN

Para la implementación se va a utilizar un Fortinet Fortigate 800D y se configurará lo siguiente:

- Configurar el LDAP para acceder al dominio del directorio activo.
- Configurar el RADIUS para la autenticación de los usuarios.
- Crear VPN Portal con un pool de ip.
- Crear los grupos de usuarios de acuerdo a su sede correspondiente.
- Crear una política de acceso remoto.
- Configurar equipos desktops.
- Configurar Forticlient VPN en los usuarios para el acceso remoto.
- Realizar pruebas de conexión.

3.2.2.3. Requerimientos y necesidades del pedido

Para la implementación se requiere como base acceso a 918 usuarios según el informe de usuarios por locales, pero al estar en un proceso de elección grande se va a contratar una cantidad considerable de personas adicional, por lo que se eligió el Fortigate 800D que tiene capacidad de hasta 5000 usuarios por acceso remoto, (Ver Figura 8).



	FORTIGATE 800D
Interfaces and Modules	
Hardware Accelerated 10 GE SFP+ Slots	2
Hardware Accelerated GE SFP Slots	8
Hardware Accelerated GE RJ45 Ports	16
Accelerated GE RJ45 Bypass Interfaces	4
GE RJ45 Management / HA Ports	2
USB Ports (Client / Server)	1 / 2
Console Port	1
Onboard Storage	1× 240 GB SSD
Included Transceivers	2× SFP (SX 1 GE)
System Performance — Enterprise Traffic Mix	
IPS Throughput [1]	4.2 Gbps
NGFW Throughput [1] [4]	4 Gbps
Threat Protection Throughput [1] [5]	3 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	36 / 36 / 22 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	33 Mpps
Concurrent Sessions (TCP)	5 Million
New Sessions/Second (TCP)	280,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) [1]	20 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	2.2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	5,000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	3.9 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	2,400
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	380,000
Application Control Throughput (HTTP 64K) [2]	9 Gbps
CAPWAP Throughput (1444 byte, UDP)	5.5 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	64
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512
Maximum Number of FortiTokens	1,000
High Availability Configurations	Active-Active, Active-Passive, Clustering

	FORTIGATE 800D
Dimensions and Power	
Height x Width x Length (inches)	1.75 × 17.0 × 15.4
Height x Width x Length (mm)	44.45 × 432 × 418
Weight	19.0 lbs (8.6 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 1 RU
Wall Mountable	No
Power Input	100–240V AC, 50/60 Hz
Power Consumption (Average / Maximum)	128 W / 187 W
Current (Maximum)	110/120, 220/240 5A
Heat Dissipation	638 BTU/h
Redundant Power Supplies	Hot-Swappable) Optional
Operating Environment and Certifications	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	55 dBA
Forced Airflow	Side to Back
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, BSMI, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

Figura 8. Características del Fortinet Fortigate 800D.
Fuente: Elaboración propia.

Además, se requiere que:

- El acceso remoto VPN este permite a todo el personal de la institución.
- El personal deberá conectarse mediante al túnel VPN con su usuario y clave de dominio.
- El acceso estará limitado solo al equipo que le corresponde dentro de la institución.
- El área tecnológica es responsable de la creación y asignación de los accesos remotos, y estos deben ser aprobados por su gerencia.

3.2.3. Fase Implementación

En esta fase se realizará desde la instalación, configuración, pruebas de la implementación hasta un manual para usuarios.

3.2.3.1. Instalación del Hardware

Se procede a la instalación del hardware Fortinet Fortigate 800D en el gabinete del centro de datos, realizando las conexiones correspondientes.

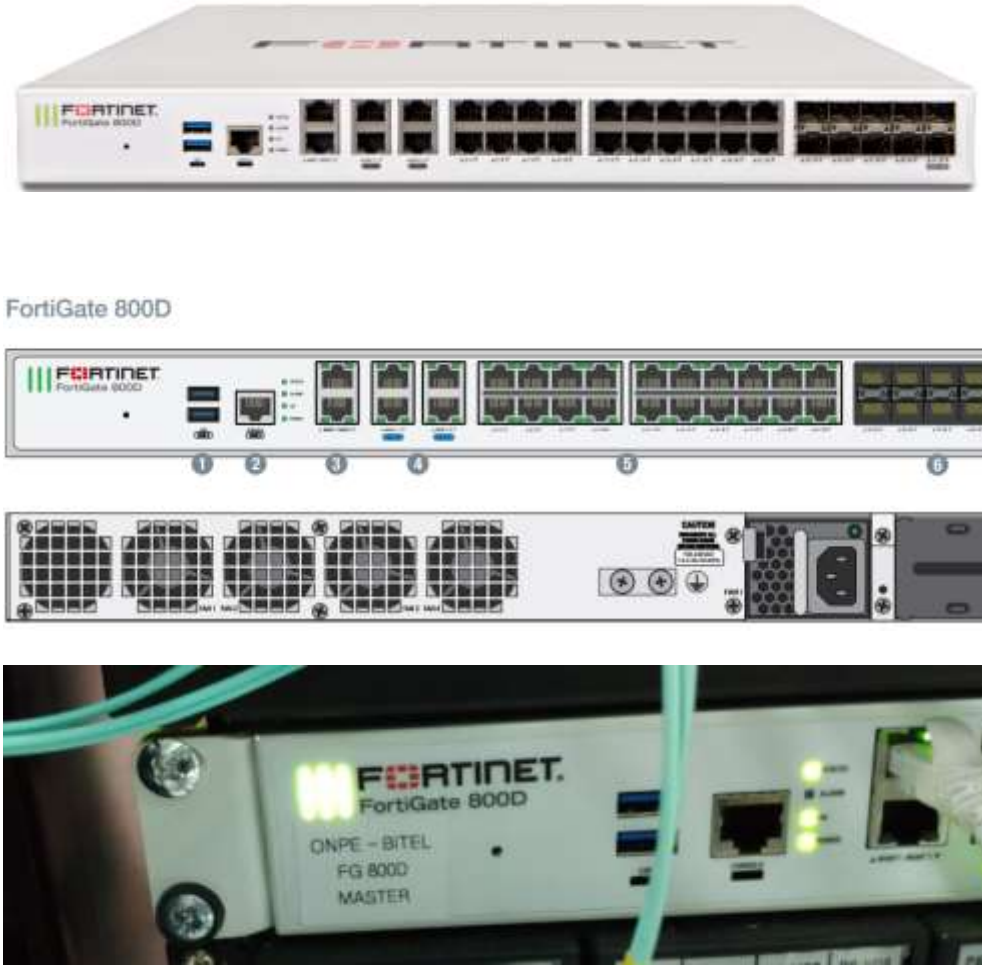


Figura 9. Fortinet Fortigate 800D.
Fuente: Elaboración propia.

3.2.3.2. Configuración del Fortinet inicial y puesta en marcha

Se procede a conectar el equipo por consola e ingresamos en login con admin y la clave por defecto.

Procedemos a cambiar el hostname con el comando:

config system global

set hostname FW-1

end

Procedemos a darle un IP para poder conectarnos a la interface

config system interface

edit internal

set ip “IP”

Una vez terminado de configurar el IP ingresamos a la interface, (Ver Figura 10).

Figura 10. Interface de inicio de sesión.
Fuente: Elaboración propia.

Ingresamos con las credenciales y verificamos el contenido, (Ver Figura 11).

Figura 11. Contenido Fortigate.
Fuente: Elaboración propia.

3.2.3.3. Configuración con autenticación Radius

Primero se procede a crear el LDAP server, para esto es necesario la ip del directorio activo e identificar el atributo que se va a consultar en este caso sAMAccountName, (Ver Figura 12).

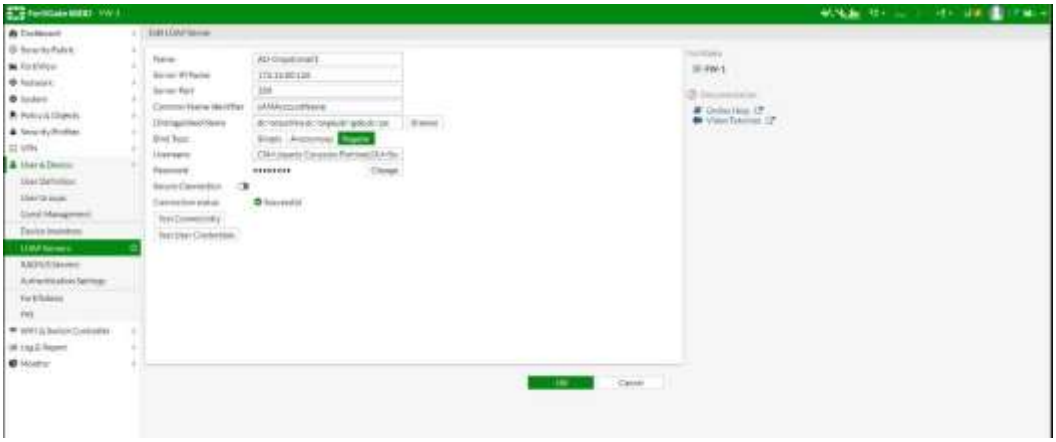


Figura 12. LDAP Server.
Fuente: Elaboración propia.

Luego procedemos a configurar el RADIUS Servers para que los usuarios puedan autenticar mediante el directorio activo, asignamos un nombre y la IP del servidor RADIUS, (Ver Figura 13).

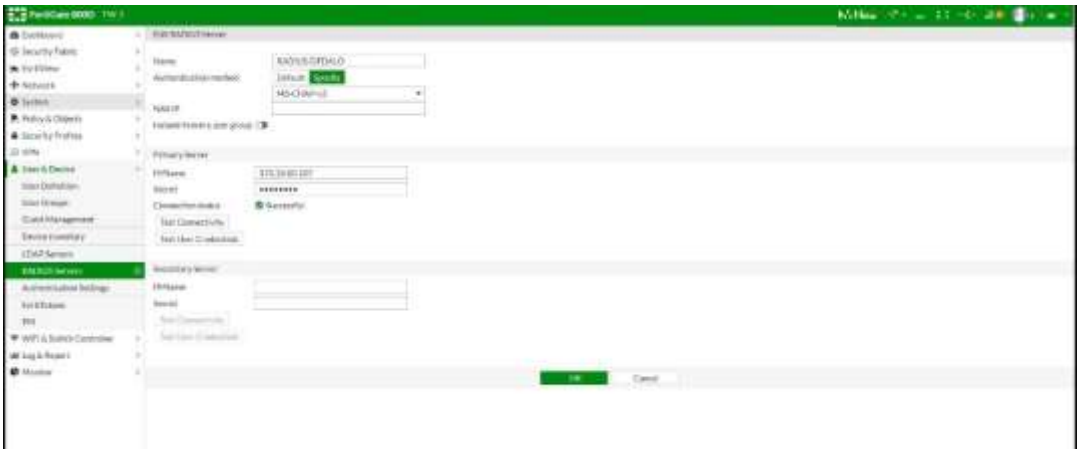


Figura 13. RADIUS Servers.
Fuente: Elaboración propia.

3.2.3.4. Configuración Firewall para autenticación y bloqueo

Primero vamos a crea el portal VPN, para esto ingresamos a VPN/SSL-VPN Portals damos un nombre, habilitamos el Tunnel Mode, en Routing Address vamos agregar a los grupos por segmento de acuerdo a la sede que se les va a permitir ingresar remotamente y en Source IP pools es el grupo de pool de ip que se le va asignar al forticlient VPN cuando se conecten, (Ver Figura 14).

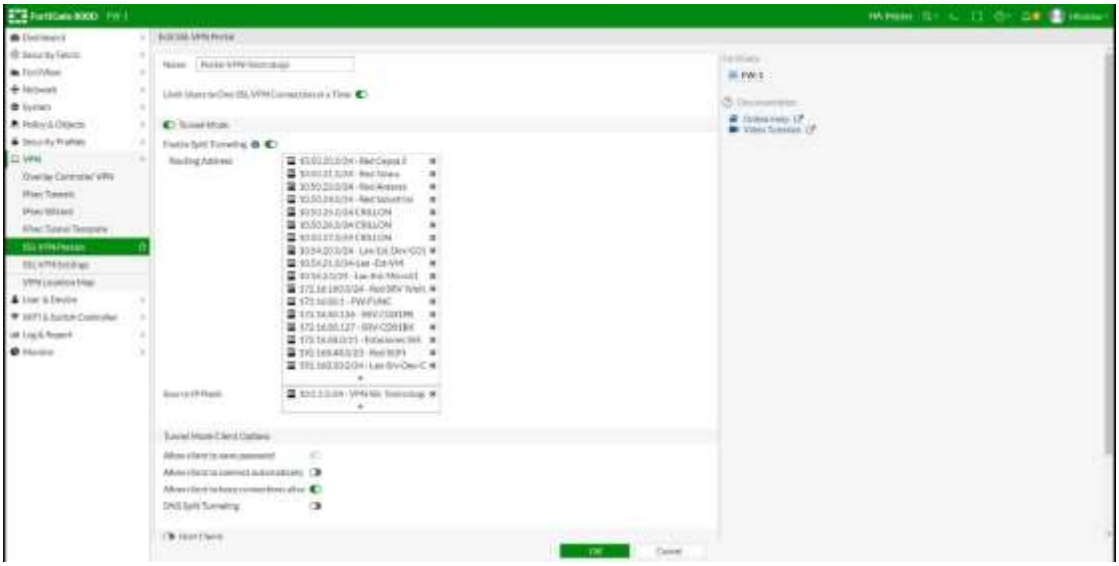


Figura 14. SSL VPN Portals.
Fuente: Elaboración propia.

Luego procedemos a configurar SSL-VPN Settings para el cual vamos a seleccionar WAN-INTERNET, el puerto 10443, el certificado del servidor len.onpe.gob.pe, en IP ranges vamos a seleccionar el pool de ip que ya hemos generado, vamos a especificar los DNS y en Authentication/Portal Mapping vamos a autorizar los grupos que deseamos que puedan ingresar, (Ver Figura 15).

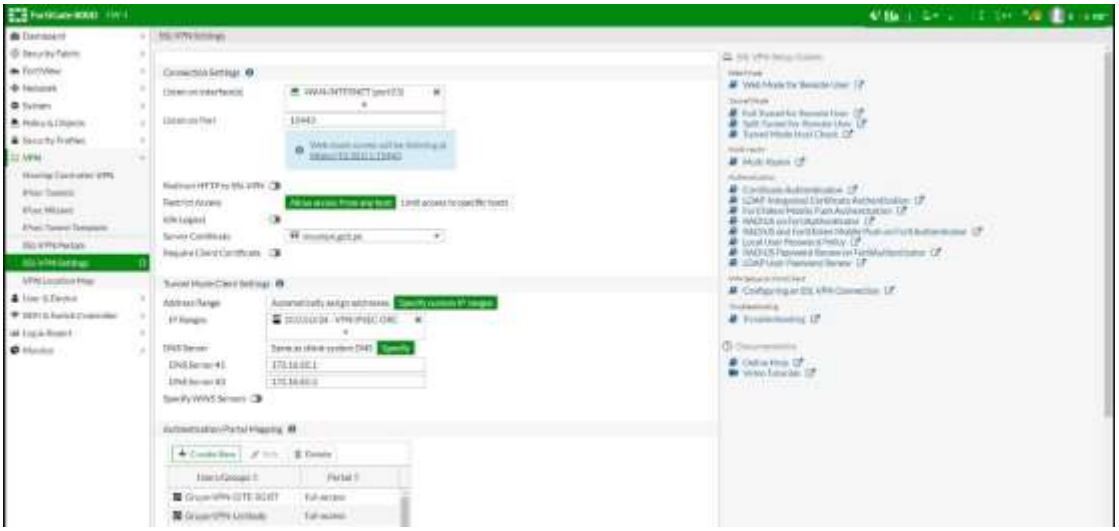


Figura 15. SSL VPN Settings.
Fuente: Elaboración propia.

Ahora procedemos a crear una política de acceso, para eso ingresamos a Policy & Objects/IPv4 Policy, creamos un nombre, seleccionamos la interface VPN que estamos usando, luego que alcance el segmento Lan, en Source solo dar permiso al pool de ip que será asignados por el forticlient VPN y en Destination vamos a dar permisos a que grupos se puede conectar, (Ver Figura 16).

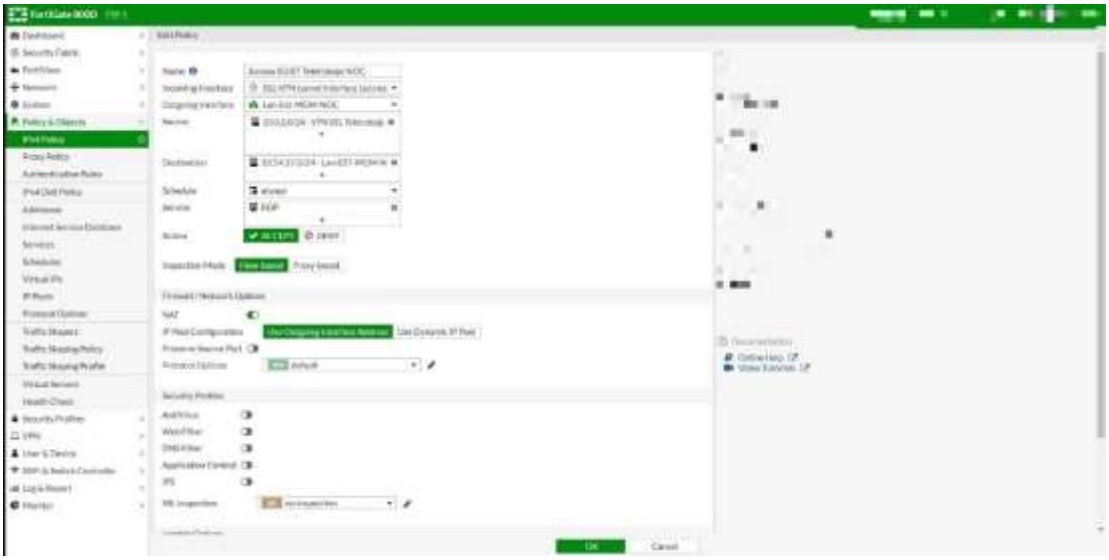


Figura 16. Política de acceso.
Fuente: Elaboración propia.

Para la creación de grupos nos dirigimos a User & Device/User Groups y podemos crear los grupos de acuerdo al requerimiento por gerencia o sede, (Ver Figura 17).

Figura 17. User Groups.
Fuente: Elaboración propia.

Por último, los usuarios en User & Device/User Definition, (Ver Figura 18).

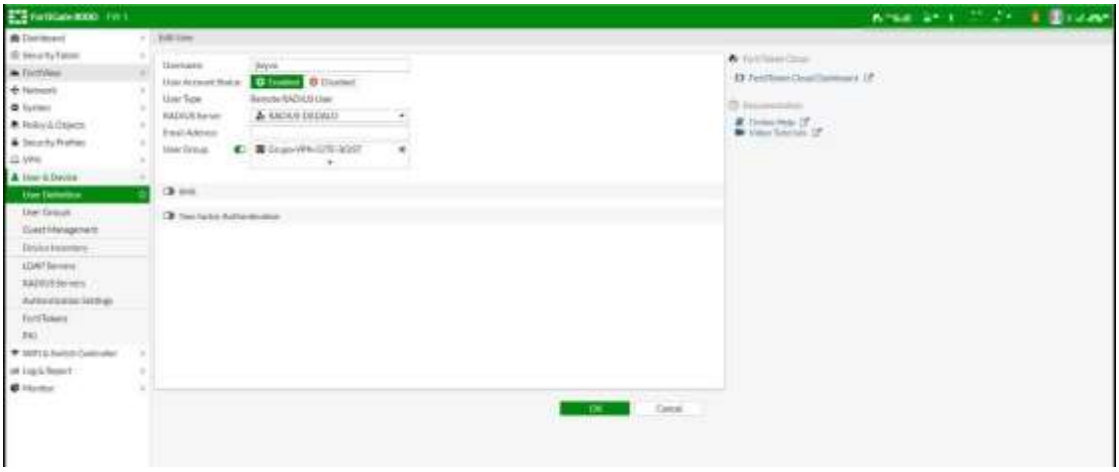


Figura 18. User Definition.
Fuente: Elaboración propia.

3.2.3.5. Configuración de equipos desktop y desactivar suspensión

Procedemos en el equipo Windows activar el acceso remoto en propiedades de sistema, acceso remoto, permitir conexiones remotas a este equipo, seleccionar usuario y agregamos al usuario correspondiente, (Ver Figura 19).

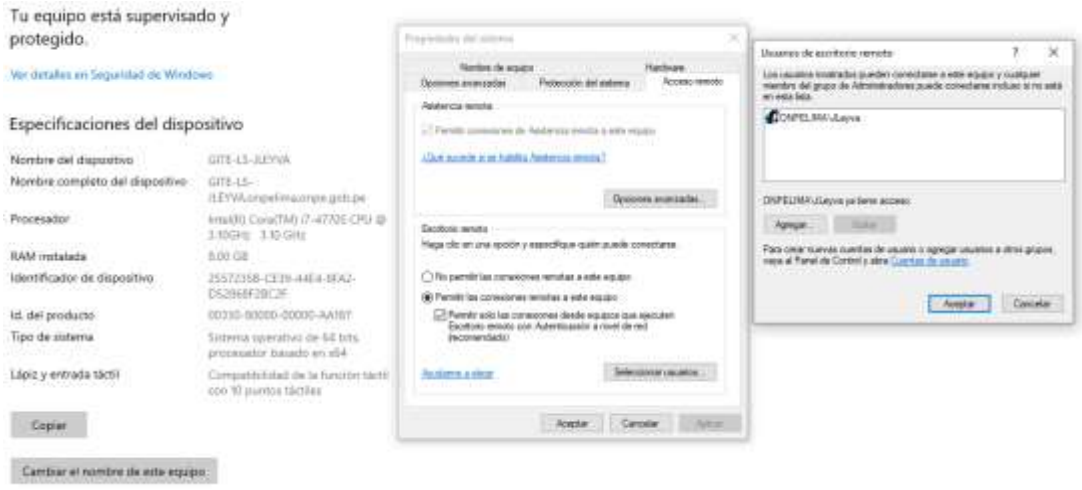


Figura 19. Configuración desktop Windows.
Fuente: Elaboración propia.

Para evitar que el equipo quede suspendido vamos a la configuración de opciones de energía y cambiamos la configuración de Apagar pantalla y Poner el equipo en estado de suspensión en Nuca, (Ver Figura 20).

Figura 20. Desactivar estado de suspensión.
Fuente: Elaboración propia.

Para un equipo Mac OS vamos a ir a la opción compartir, seleccionamos compartir pantalla, permitir acceso a: Solo estos usuarios, damos clic en más y agregamos al usuario, (Ver Figuras 21 y 22).

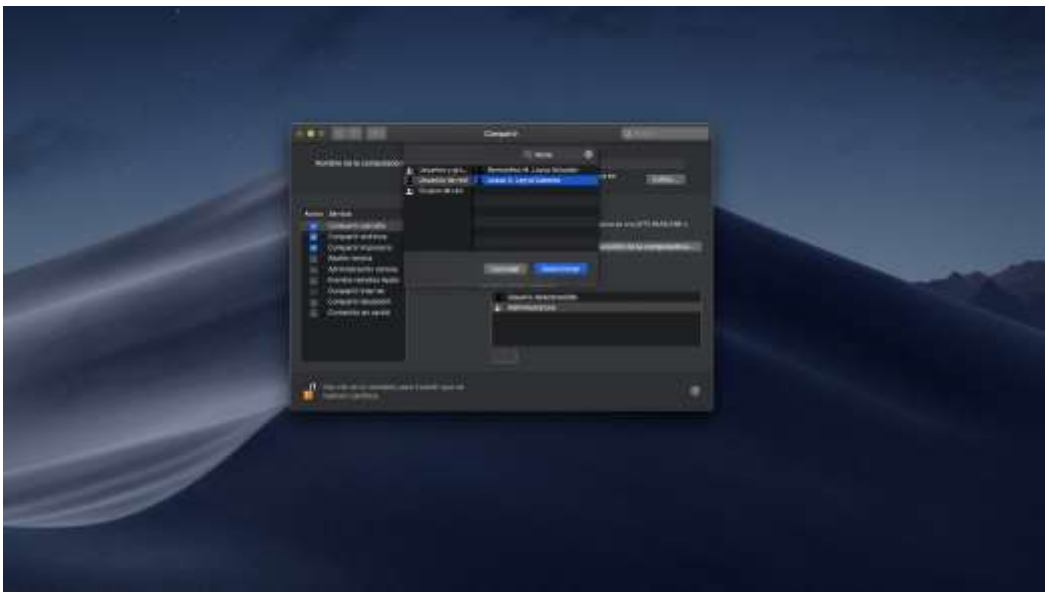


Figura 21. Configuración desktop Mac OS.
Fuente: Elaboración propia.

Figura 22. Agregar usuario de dominio en Mac OS
Fuente: Elaboración propia.

3.2.3.6. Instalación de forticlient VPN y token

Descargamos y ejecutamos el aplicativo FortiClientVPNOnlineInstaller_6.4, (Ver Figura 23).

Figura 23. Instalación Forticlient VPN (1).
Fuente: Elaboración propia.

Le damos siguiente e instalar, (Ver Figura 24).

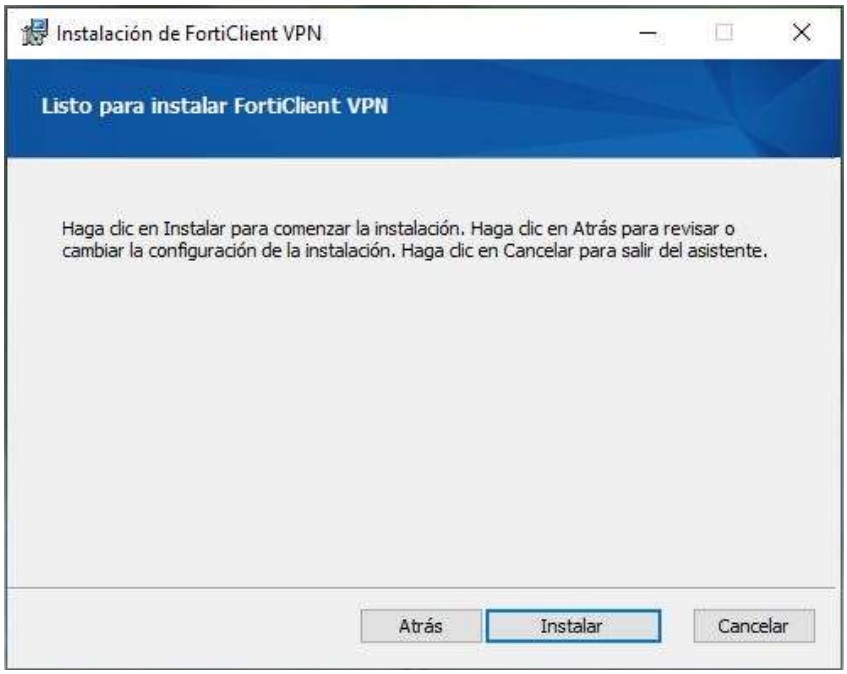


Figura 24. Instalación Forticlient VPN (2).
Fuente: Elaboración propia.

Una vez instalado abrimos el aplicativo y le damos en Configure VPN tal, (Ver Figura 25).

Figura 25. Instalación Forticlient VPN (3).
Fuente: Elaboración propia.

En Connection Name colocamos un nombre para esta configuración, en Remoto Gateway ingresamos len.onpe.gob.pe, puerto 10443 y si quieren guardar el usuario darle check en Save login, (Ver Figura 26).

Figura 26. Instalación Forticlient VPN (4).
Fuente: Elaboración propia.

Luego procedemos a conectarnos con las credenciales de la cuenta del directorio activo, (Ver Figura 27).

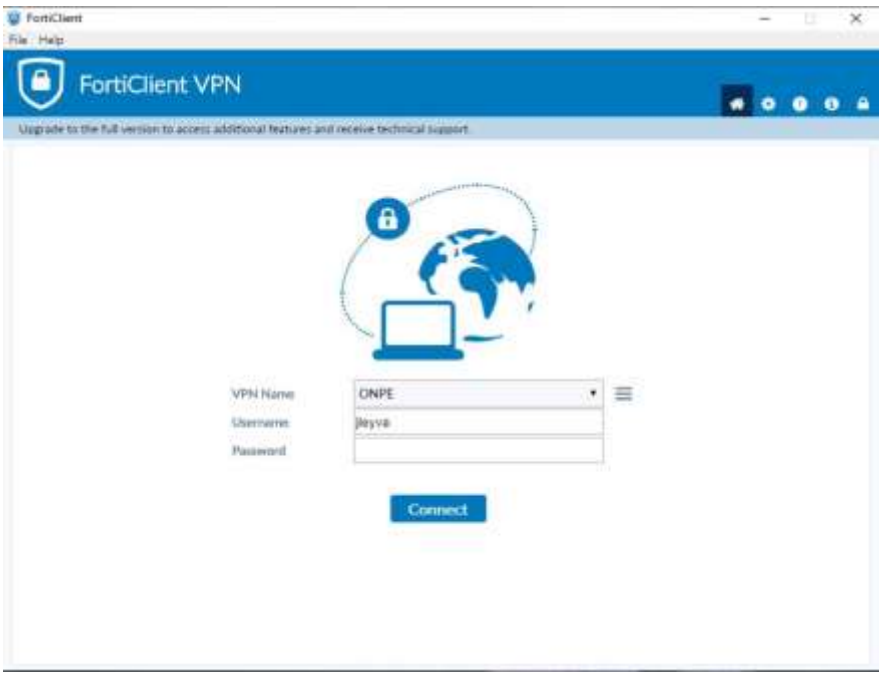


Figura 27. Instalación Forticlient VPN (5).
Fuente: Elaboración propia.

Para algunos usuarios se le pedirá que ingrese el número de token al ingresar que es una seguridad adicional, este token se le asignara al usuario específico así lo requiera, (Ver Figura 28).

Figura 28. Token Fortinet.
Fuente: Elaboración propia.

3.2.3.7. Pruebas de la red

Ya habiendo establecido la conexión con el forticlient VPN ingresamos para Windows a Conexión a Escritorio remoto con la ip del equipo al que estamos autorizados ingresar, (Ver Figura 29).

Figura 29. Conexión a Escritorio remoto.
Fuente: Elaboración propia.

Ingresamos las credenciales de la cuenta del directorio activo, (Ver Figura 30).

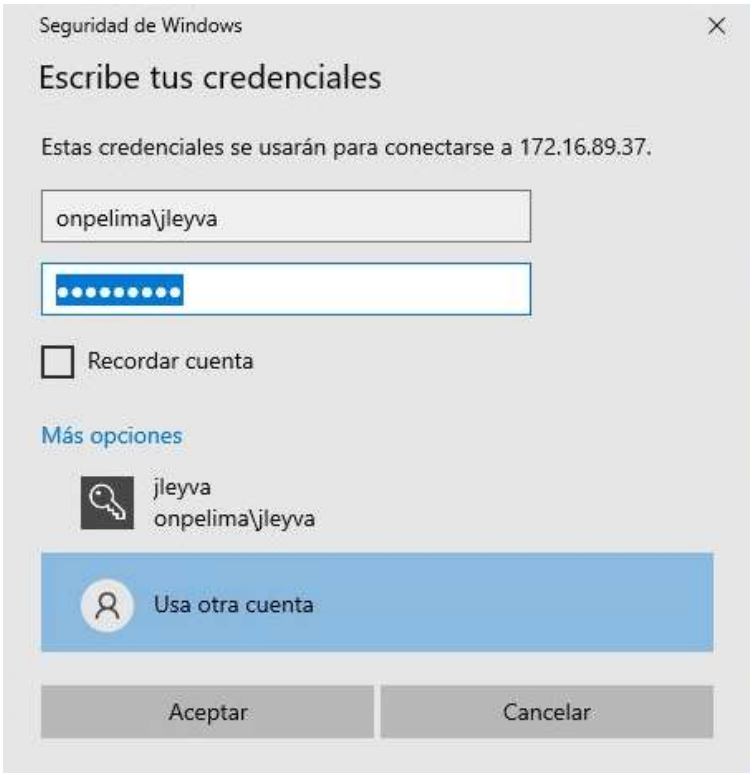


Figura 30. Credenciales de dominio para ingreso a Windows.
Fuente: Elaboración propia.

Finalmente, en Aceptar e ingresamos al equipo, (Ver Figura 31).

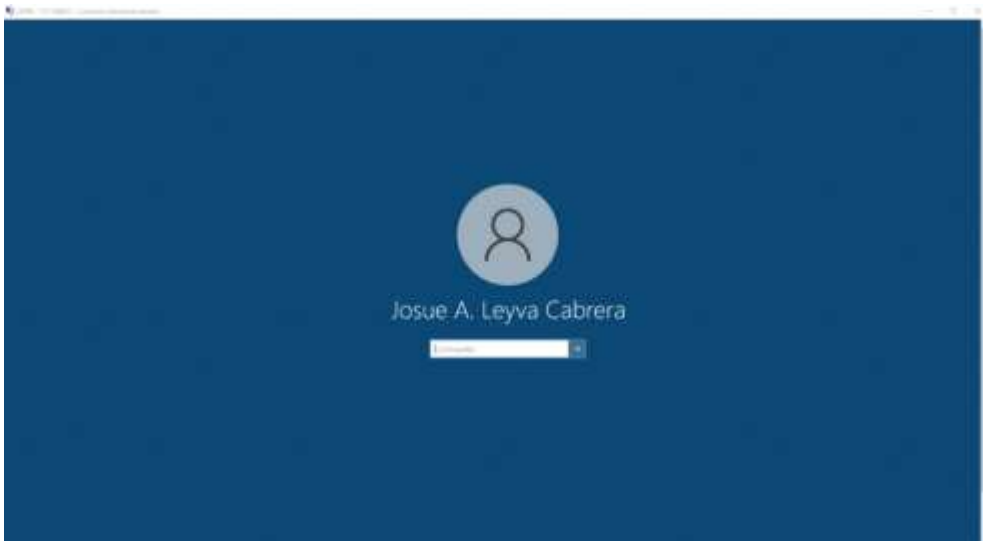


Figura 31. Ingreso remoto a Windows.
Fuente: Elaboración propia.

Para una Mac OS vamos a instalar el VNCViewer, lo ejecutamos y colocamos la ip, (Ver Figura 32).

Figura 32. VNCViewer.
Fuente: Elaboración propia.

Luego procedemos a ingresar las credenciales de la cuenta del directorio activo, (Ver Figura 33).

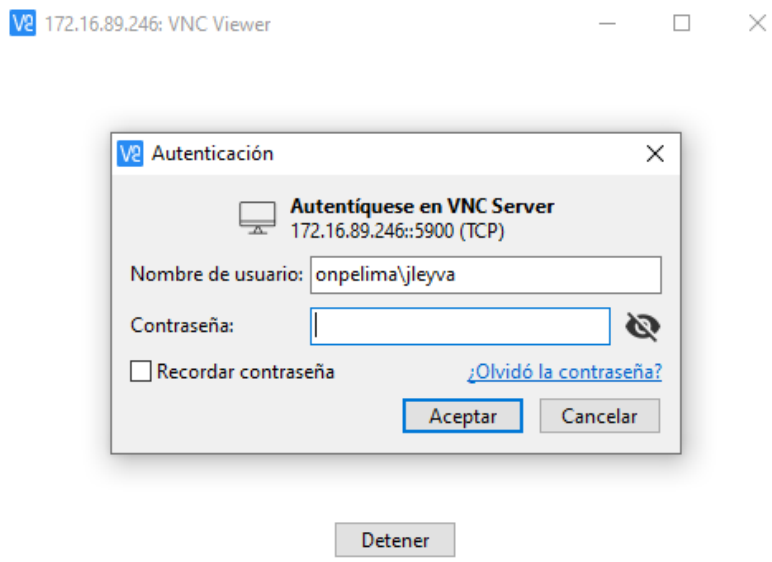


Figura 33. Credenciales de dominio para ingreso a VNCViewer.
Fuente: Elaboración propia.

Luego ingresamos nuevamente con las credenciales, (Ver Figura 34).

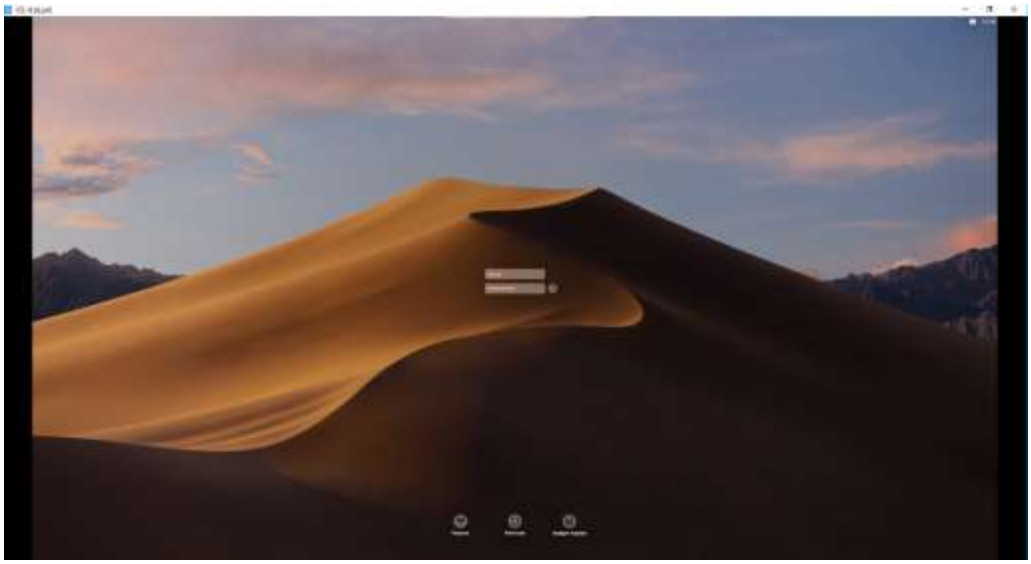


Figura 34. Credenciales de dominio para ingreso a Mac OS.
Fuente: Elaboración propia.

Finalmente, ya estamos dentro del equipo, (Ver Figura 35).

Figura 35. Ingreso remoto a Mac OS.
Fuente: Elaboración propia.

Podemos validar el ingreso del usuario en este caso jleyva en el Fortigate en la opción Monitor/SSL-VPN Monito, (Ver Figura 36).

Figura 36. Validación de acceso remoto en el Monitor del Fortigate.
Fuente: Elaboración propia.

3.2.3.8. Manual de configuración VPN para usuarios

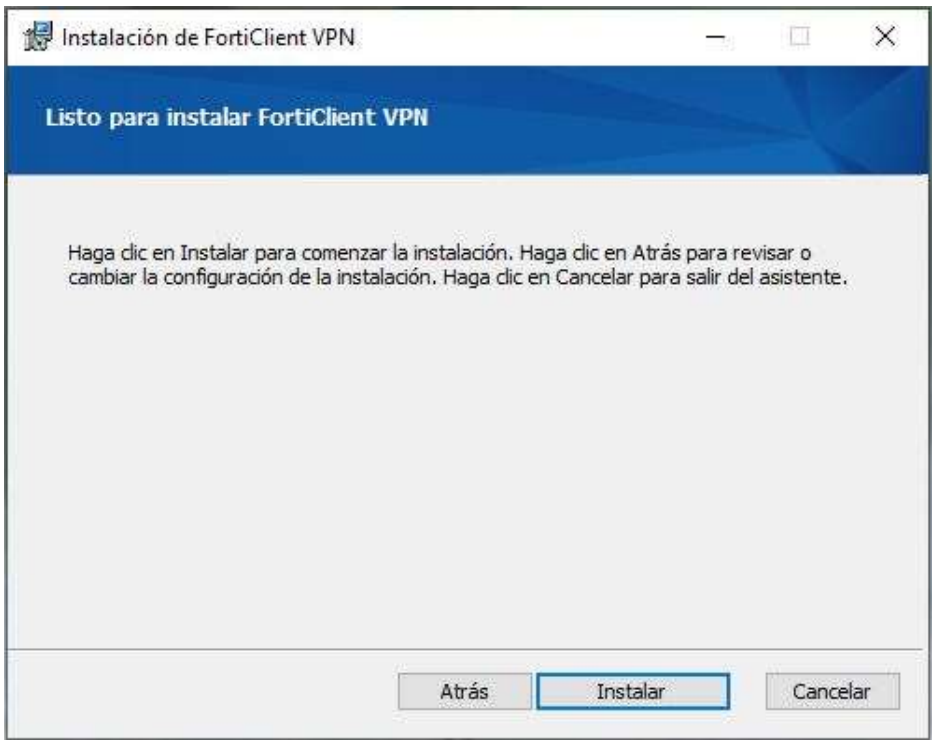
En esta sección vamos a realizar un manual de la configuración VPN para aquellos que por uno u otro motivo cambiaron de equipo personal y necesitan volver a configurar el forticlient VPN.

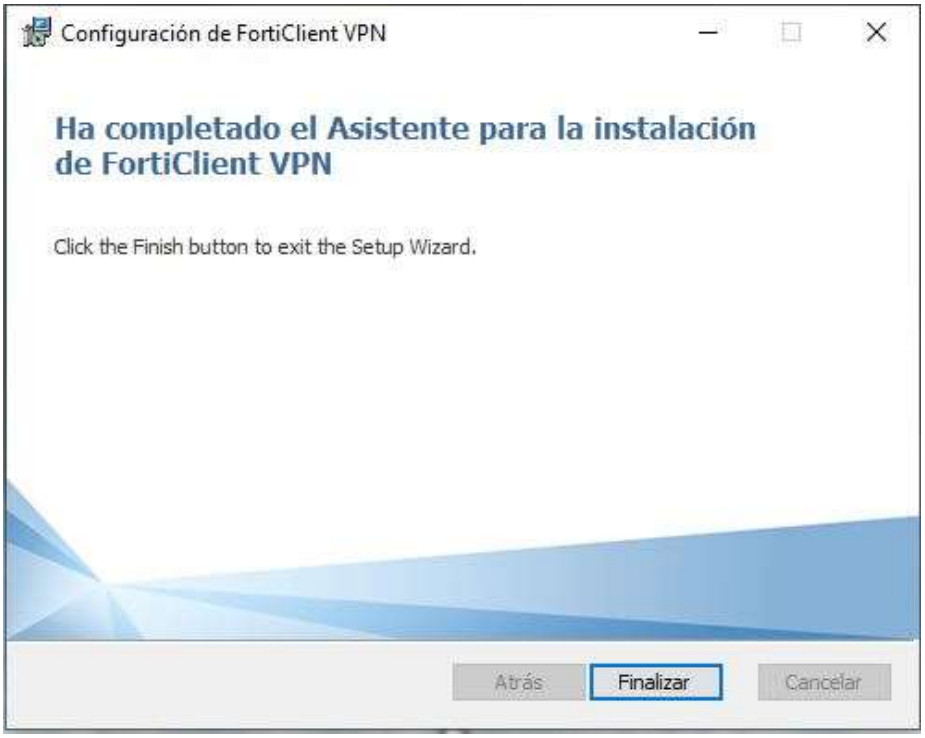
Primero descargamos el aplicativo desde el siguiente link:

https://www.forticlient.com/downloads

Hacemos clic en Download for Windows o Mac según el sistema operativo.

Instalamos el aplicativo como.





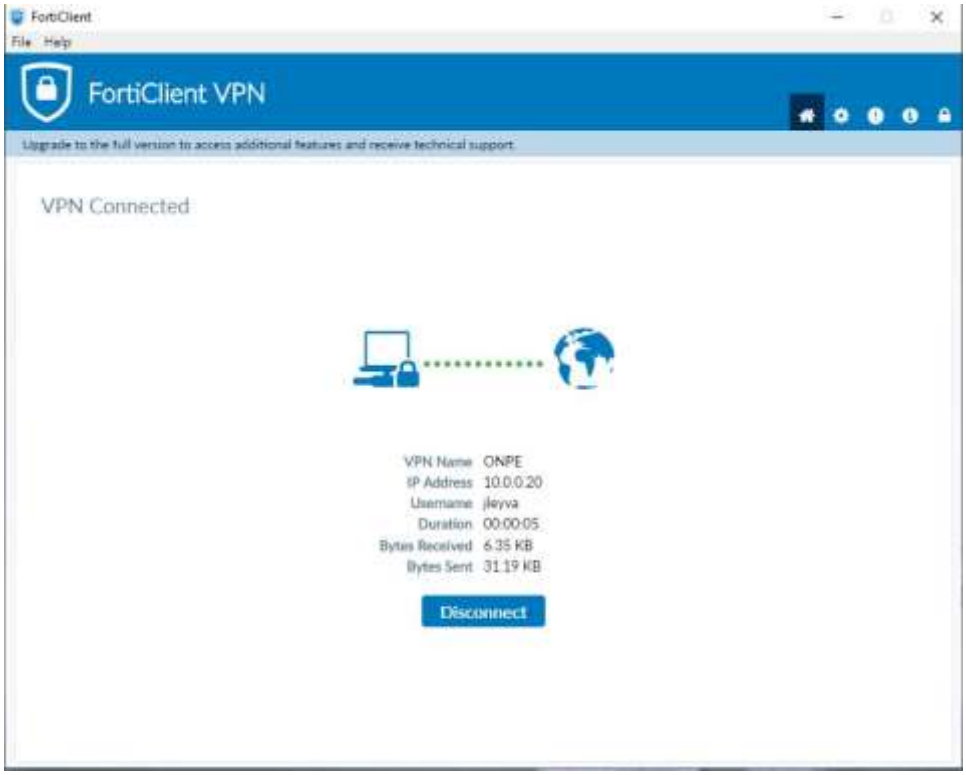
Accedemos al aplicativo

Hacemos clic en configurar VPN

Configuramos los siguientes datos: Remoto Gateway ingresamos len.onpe.gob.pe, puerto: 10443, tipo de conexión SSL y damos clic en save.

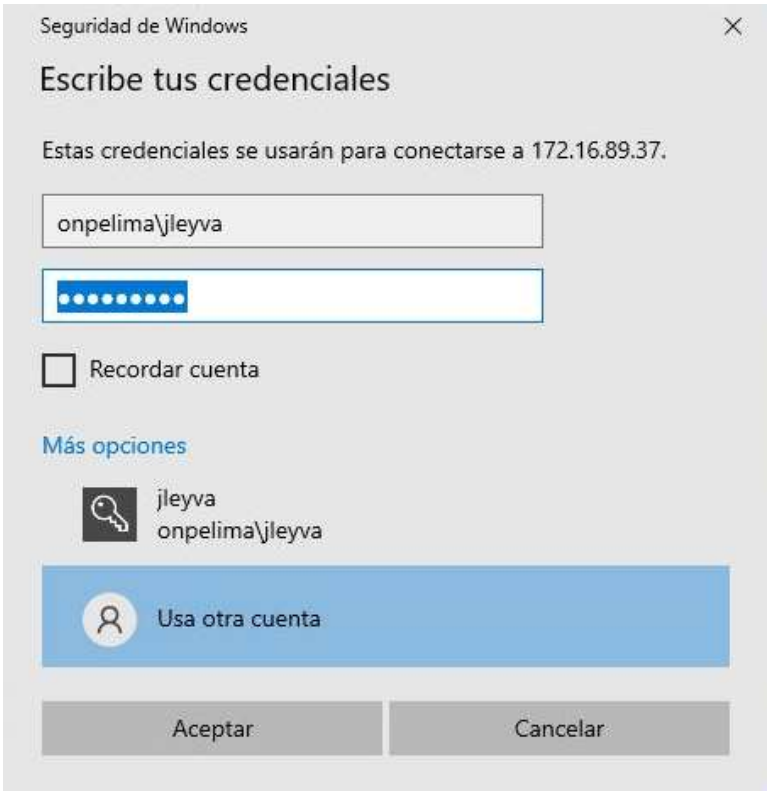
Colocamos el nombre de usuarios y contraseña, se puede guardar las credenciales dando clic en save password y damos clic en Connect.

La conexión se encuentra establecida



Luego ingresamos al escritorio remoto y digitamos nuestra IP del equipo institucional, la ip será enviada a su correo.

Finalmente ingresamos dominio, usuarios de red y contraseña



CAPITULO 4

RESULTADOS

4.1. Resultados

Para la obtención de resultados se llevó a cabo cada una de las fases planificadas, logrando la implementación de la VPN, se realizó una serie de configuraciones en el que se definió la política de acceso remoto a la red para el personal de la institución, siendo estos satisfactorios, (Ver Figura 37).

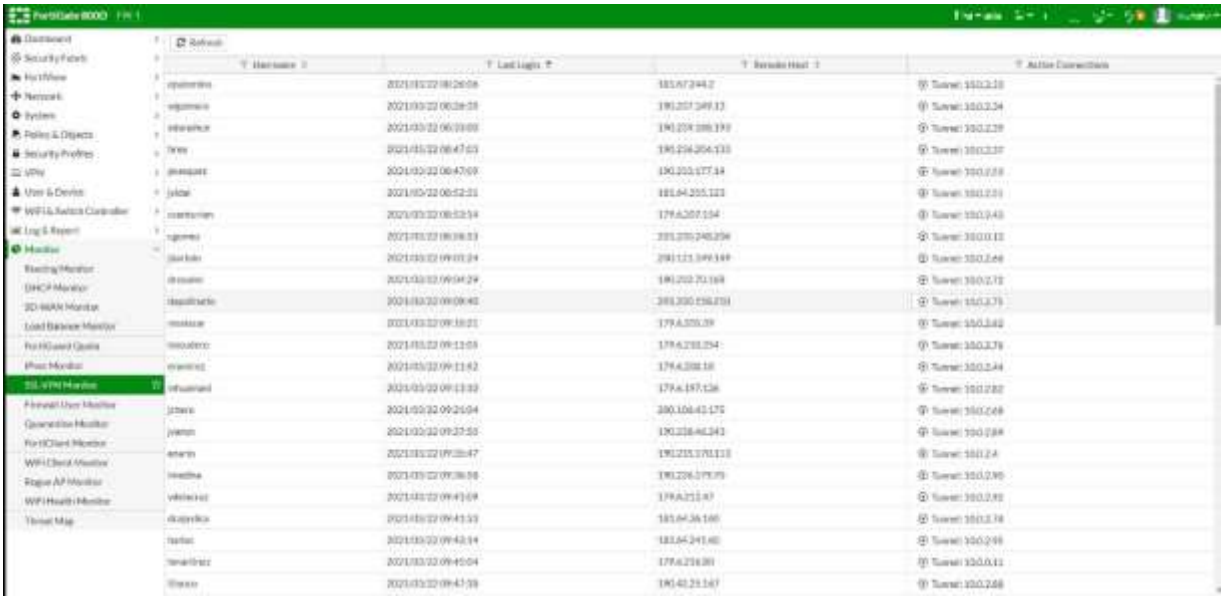


Figura 37. Validación de acceso remoto para el personal de ONPE.
Fuente: Elaboración propia.

4.2. Presupuesto

En esta sección se presenta el registro de todos los ingresos y egresos a la caja a lo largo del tiempo del proyecto, (Ver Tabla 5).

Tabla 5. Flujo de Caja.

Flujo de Caja						
	Mes 1	**Mes 2**	**Mes 3**	**Mes 4**	**Mes 5**	**Mes 6**
Ingresos						
Venta/Beneficios	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Egresos						
Recursos Humanos						
Jefe de Proyecto	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00	S/. 9,000.00
Ingeniero de redes	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00
2 técnicos en redes	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00	S/. 8,000.00
2 soporte Técnico	S/. 0.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00	S/. 6,000.00
Equipo de Computo						
Fortinet fortigate 800d	S/. 18,200.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Mantenimiento del Fortinet	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 8,000.00
Total	**S/. 41,200.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 29,000.00**	**S/. 37,000.00**
Total Acumulado	**S/. 41,200.00**	**S/. 70,200.00**	**S/. 99,200.00**	**S/. 128,200.00**	**S/. 157,200.00**	**S/. 194,200.00**

Fuente: Elaboración propia.

Como resultado para la implementación se presupuestó S/. 194,200.00.

CONCLUSIONES

Al término del proyecto se puede concluir que los objetivos fueron alcanzados exitosamente, la implementación de la VPN garantizo la integridad del personal de la institución estando en un estado de emergencia por COVID-19, permitiéndoles seguir con su cronograma de actividades y no viéndose afectado las elecciones internas 2020 y las elecciones generales 2021.

Se definió una política de acceso remoto a la red de la institución, en la cual el uso apropiado de la conexión remota VPN permite el ingreso a la red y acceder a su equipo autorizado, se aplica a todo el personal de la ONPE.

La arquitectura utilizada en la implementación permite la conectividad vía VPN SSL, es decir que mediante el túnel VPN utilizando el Forticlient VPN se le asigna una ip autorizado para ingresar a la red institucional y esto puede ser monitoreado en el Fortigate para auditoria.

Se instalo y configuro a todo el personal de la institución el Forticlient VPN para el uso de teletrabajo, dando soporte técnico satisfactoriamente y así cuidando su integridad.

Finalmente se desarrolló un manual para la instalación del Forticlient VPN para el personal de la institución, indicando los pasos a realizar para conexión remota de acceso remoto que por uno u otro motivo cambiaron de equipo personal y necesitan volver a configurar el forticlient VPN.

RECOMENDACIONES

Realizar auditoria de las conexiones VPN a través del Monitor del Fortigate 800D.

Mantener el firmware del Fortigate actualizado para evitar posibles bugs.

Realizar un mantenimiento al Fortinet cada 6 meses.

Se recomienda que los equipos personales del personal cuenten con antivirus actualizado.

BIBLIOGRAFÍAS

Tesis

Mar, J. (2016). Propuesta de implementación de una intranet vía VPN para mejorar la confidencialidad del intercambio de información entre las sedes Lima – Cusco del INEI. Universidad Andina del Cusco, Facultad de Ingeniería y Arquitectura, Perú.

Ramírez, D., Jota, Y., y Penagos, A. (2019). Diseño de una red privada virtual (VPN) con seguridad L2pt para la empresa laboratorios EXPOFARMA S.A. Universidad Cooperativa de Colombia, Facultad de Ingeniería, Colombia.

Peña, D. (2016). Diseño e implementación de una red privada virtual (VPN SSL) utilizando el método de autenticación LDAP en una empresa privada. Universidad Central de Venezuela, Facultad de Ingeniería de Comunicaciones y Redes, Venezuela.

Libros

Sampieri, H. (2017). *Metodología De La Investigación (6ta Edición)*. Recuperado de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Recursos electrónicos

Citrix (21-11-2019). Citrix Systems: México. Recuperado de https://www.citrix.com/es-mx/glossary/what-is-remote-access.html

Expressvpn (01-03-2016). Beneficios y ventajas de las VPN. Recuperado de https://www.expressvpn.com/es/what-is-vpn

Ciberseguridad (16-03-2021). Acceso remoto Seguro. Recuperado de https://ciberseguridad.com/guias/acceso-remoto-seguro/

Argentina (17-03-2020). ¿Qué es el teletrabajo? Recuperado de https://www.argentina.gob.ar/trabajo/teletrabajo/que-es

Economipedia (02-05-2020). Teletrabajo. Recuperado de https://economipedia.com/definiciones/teletrabajo.html

Vertical-ibérica (19-02-2020). Qué es Fortinet y cómo funciona. Recuperado de https://vertical-iberica.com/que-es-fortinet-y-como-funciona/

Z-net (10-03-2019) Tutorial Fortinet: ¿Por qué Fortigate? Recuperado de https://www.z-net.com.ar/blog-post/1-tutorial-fortinet-por-que-fortigate/